



# Citrix NetScaler Administration Guide

## Copyright and Trademark Notice

© CITRIX SYSTEMS, INC., 2012. ALL RIGHTS RESERVED. NO PART OF THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS OR USED TO MAKE DERIVATIVE WORK (SUCH AS TRANSLATION, TRANSFORMATION, OR ADAPTATION) WITHOUT THE EXPRESS WRITTEN PERMISSION OF CITRIX SYSTEMS, INC.

ALTHOUGH THE MATERIAL PRESENTED IN THIS DOCUMENT IS BELIEVED TO BE ACCURATE, IT IS PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE ALL RESPONSIBILITY FOR THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS MANUAL.

CITRIX SYSTEMS, INC. OR ITS SUPPLIERS DO NOT ASSUME ANY LIABILITY THAT MAY OCCUR DUE TO THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS DOCUMENT. INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. COMPANIES, NAMES, AND DATA USED IN EXAMPLES ARE FICTITIOUS UNLESS OTHERWISE NOTED.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler appliance. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

BroadCom is a registered trademark of BroadCom Corporation. Fast Ramp, NetScaler, and NetScaler Request Switch are trademarks of Citrix Systems, Inc. Linux is a registered trademark of Linus Torvalds. Internet Explorer, Microsoft, PowerPoint, Windows and Windows product names such as Windows NT are trademarks or registered trademarks of the Microsoft Corporation. NetScape is a registered trademark of Netscape Communications Corporation. Red Hat is a trademark of Red Hat, Inc. Sun and Sun Microsystems are registered trademarks of Sun Microsystems, Inc. Other brand and product names may be registered trademarks or trademarks of their respective holders.

Software covered by the following third party copyrights may be included with this product and will also be subject to the software license agreement: Copyright 1998 © Carnegie Mellon University. All rights reserved. Copyright © David L. Mills 1993, 1994. Copyright © 1992, 1993, 1994, 1997 Henry Spencer. Copyright © Jean-loup Gailly and Mark Adler. Copyright © 1999, 2000 by Jef Poskanzer. All rights reserved. Copyright © Markus Friedl, Theo de Raadt, Niels Provos, Dug Song, Aaron Campbell, Damien Miller, Kevin Steves. All rights reserved. Copyright © 1982, 1985, 1986, 1988-1991, 1993 Regents of the University of California. All rights reserved. Copyright © 1995 Tatu Ylonen, Espoo, Finland. All rights reserved. Copyright © UNIX System Laboratories, Inc. Copyright © 2001 Mark R V Murray. Copyright 1995-1998 © Eric Young. Copyright © 1995, 1996, 1997, 1998. Lars Fenneberg. Copyright © 1992. Livingston Enterprises, Inc. Copyright © 1992, 1993, 1994, 1995. The Regents of the University of Michigan and Merit Network, Inc. Copyright © 1991-2, RSA Data Security, Inc. Created 1991. Copyright © 1998 Juniper Networks, Inc. All rights reserved. Copyright © 2001, 2002 Networks Associates Technology, Inc. All rights reserved. Copyright (c) 2002 Networks Associates Technology, Inc. Copyright 1999-2001 © The Open LDAP Foundation. All Rights Reserved. Copyright © 1999 Andrzej Bialecki. All rights reserved. Copyright © 2000 The Apache Software Foundation. All rights reserved. Copyright (C) 2001-2003 Robert A. van Engelen, Genivia inc. All Rights Reserved. Copyright (c) 1997-2004 University of Cambridge. All rights reserved. Copyright (c) 1995. David Greenman. Copyright (c) 2001 Jonathan Lemon. All rights reserved. Copyright (c) 1997, 1998, 1999. Bill Paul. All rights reserved. Copyright (c) 1994-1997 Matt Thomas.

---

All rights reserved. Copyright © 2000 Jason L. Wright. Copyright © 2000 Theo de Raadt. Copyright © 2001 Patrik Lindergrén.

All rights reserved.

Last Updated: March 2012

Document code: May 21 2012 05:40:33

---



---

# Contents

<b>Preface</b> .....	<b>17</b>
Formatting Conventions for NetScaler Documentation .....	17
Documentation Available on the NetScaler Appliance .....	18
Getting Service and Support .....	19
NetScaler Documentation Feedback .....	19
<b>1 Authentication and Authorization</b> .....	<b>21</b>
Configuring Users and Groups.....	22
Configuring User Accounts.....	22
To create a user account by using the NetScaler command line.....	22
To modify or remove a user account by using the NetScaler command line.....	23
Parameters for configuring a user account.....	23
To configure a user account by using the configuration utility.....	24
Configuring User Groups.....	24
To create a user group by using the NetScaler command line.....	24
To modify or remove a user group by using the NetScaler command line .....	25
To bind a user to a group by using the NetScaler command line.....	25
To unbind a user from a group by using the NetScaler command line.....	25
Parameters for configuring a user group .....	26
To configure a user group by using the configuration utility.....	26
Configuring Command Policies.....	27
Built-in Command Policies.....	27
Creating Custom Command Policies.....	28
To create a command policy by using the NetScaler command line.....	30
To modify or remove a command policy by using the NetScaler command line .....	30
Parameters for configuring a command policy.....	30
To configure a command policy by using the configuration utility.....	31
Binding Command Policies to Users and Groups.....	31
To bind command policies to a user by using the NetScaler command line.....	32
To unbind command policies from a user by using the NetScaler command line.....	32

Parameters for binding a command policy to a user.....	32
To bind command policies to a user by using the configuration utility.....	32
To bind command policies to a group by using the NetScaler command line .....	33
To unbind command policies from a group by using the NetScaler command line.....	33
Parameters for binding a command policy to a group .....	33
To bind command policies to a group by using the configuration utility.....	34
Resetting the Default Administrator (nsroot) Password.....	34
To reset the nsroot password.....	34
Example of a User Scenario.....	35
Configuration steps.....	36
Configuring External User Authentication.....	37
Configuring LDAP Authentication.....	38
To configure LDAP authentication by using the configuration utility.....	40
Determining attributes in the LDAP directory.....	41
Configuring RADIUS Authentication.....	42
To configure RADIUS authentication by using the configuration utility.....	42
Choosing RADIUS authentication protocols.....	42
Configuring IP address extraction.....	43
Configuring TACACS+ Authentication.....	44
To configure TACACS+ authentication by using the configuration utility.....	44
Configuring NT4 Authentication.....	44
To configure NT4 authentication by using the configuration utility.....	45
Binding the Authentication Policies to the System Global Entity.....	45
To bind an authentication policy globally by using the configuration utility.....	45
To unbind a global authentication policy by using the configuration utility.....	45
<b>2 SNMP.....</b>	<b>47</b>
Importing MIB Files to the SNMP Manager and Trap Listener.....	48
To import the MIB files to the SNMP manager and trap listener.....	48
Configuring the NetScaler to Generate SNMPv1 and SNMPv2 Traps.....	48
Enabling or Disabling an SNMP Alarm.....	49
To enable or disable an SNMP alarm by using the command line.....	49
To enable or disable an SNMP alarm by using the configuration utility.....	49
Configuring Alarms.....	50
To configure an SNMP alarm by using the command line.....	50
Parameters for configuring SNMP alarms.....	50
To configure SNMP alarms by using the configuration utility.....	51

---

Configuring Traps.....	51
To add an SNMP trap by using the NetScaler command line.....	51
Parameters for configuring SNMP traps .....	52
To configure SNMP Traps by using the configuration utility .....	52
Enabling Unconditional SNMP Trap Logging.....	53
To enable or disable unconditional SNMP trap logging by using the NetScaler command line.....	53
Parameters for unconditional SNMP trap logging .....	54
To enable or disable unconditional SNMP trap logging by using the configuration utility.....	54
Configuring the NetScaler for SNMP v1 and v2 Queries.....	54
Specifying an SNMP Manager.....	54
To add an SNMP manager by using the NetScaler command line.....	55
To add an SNMP manager by specifying its IP address, using the NetScaler command line.....	55
To add an SNMP manager by specifying its host name, using the NetScaler command line.....	56
Parameters for configuring an SNMP manager .....	56
To add an SNMP manager by using the configuration utility .....	57
Specifying an SNMP Community.....	58
To specify an SNMP community by using the NetScaler command line .....	58
Parameters for configuring an SNMP community string .....	58
To configure an SNMP community string by using the configuration utility .....	58
To remove an SNMP community string by using the configuration utility.....	59
Configuring SNMP Alarms for Rate Limiting.....	59
Configuring an SNMP Alarm for Throughput or PPS.....	59
To configure an SNMP alarm for the throughput rate by using the NetScaler command line .....	60
To modify or remove the threshold values by using the NetScaler command line .....	60
To modify or remove the threshold values by using the NetScaler command line .....	61
Parameters for configuring an SNMP alarm for throughput or PPS .....	61
To configure an SNMP alarm for throughput or PPS by using the configuration utility .....	62
Configuring SNMP Alarm for Dropped Packets.....	62
To configure an SNMP alarm for packets dropped because of excessive throughput, by using the NetScaler command line .....	62

	To configure an SNMP alarm for packets dropped because of excessive PPS, by using the NetScaler command line .....	62
	Parameters for configuring an SNMP alarm for dropped packets.....	63
	To configure an SNMP alarm for dropped packets by using the configuration utility .....	63
	Configuring the NetScaler for SNMPv3 Queries.....	63
	Setting the Engine ID.....	64
	To set the engine ID by using the NetScaler command line.....	65
	Parameters for setting the engine ID .....	65
	To set the engine ID by using configuration utility .....	65
	Configuring a View.....	65
	To add an SNMP view by using the NetScaler command line.....	65
	Parameters for configuring an SNMP view .....	66
	To configure an SNMP view by using the configuration utility .....	66
	Configuring a Group.....	66
	To add an SNMP group by using the NetScaler command line.....	66
	Parameters for configuring an SNMP group .....	67
	To configure an SNMP group by using the configuration utility .....	67
	Configuring a User.....	67
	To configure a user by using the NetScaler command line.....	67
	Parameters for configuring an SNMP user .....	68
	To configure an SNMP user by using the configuration utility .....	68
<b>3</b>	<b>Audit Logging.....</b>	<b>71</b>
	Configuring the NetScaler Appliance for Audit Logging.....	73
	Configuring Audit Servers.....	73
	To configure a SYSLOG server action by using the command line.....	73
	To configure an NSLOG server action by using the command line.....	74
	Parameters for configuring auditing servers .....	74
	Log levels defined.....	75
	To configure an auditing server action.....	76
	Configuring Audit Policies.....	76
	To configure a SYSLOG policy by using the command line.....	76
	To configure an NSLOG policy by using the command line.....	77
	Parameters for configuring audit policies .....	77
	To configure an audit server policy.....	78
	Binding the Audit Policies Globally.....	78
	To configure a SYSLOG policy by using the command line.....	78
	Parameters for binding the audit policies globally.....	78



To globally bind the audit policy.....	79
Configuring Policy-Based Logging.....	79
Pre Requisites.....	79
Configuring an Audit Message Action.....	79
Binding Audit Message Action to a Policy.....	81
Installing and Configuring the NSLOG Server.....	81
Installing NSLOG Server on the Linux Operating System.....	82
To install the NSLOG server package on a Linux operating system.....	82
To uninstall the NSLOG server package on a Linux operating system.....	83
Installing NSLOG Server on the FreeBSD Operating System.....	83
To download NSLOG package from www.Citrix.com.....	83
To install the NSLOG server package on a FreeBSD operating system.....	84
To uninstall the NSLOG server package on a FreeBSD operating system.....	84
Installing NSLOG Server Files on the Windows Operating System.....	84
To download NSLOG package from www.Citrix.com.....	85
To install NSLOG server on a Windows operating system.....	85
To uninstall the NSLOG server on a Windows operating system.....	86
NSLOG Server Command Options.....	86
Adding the NetScaler Appliance IP Addresses on the NSLOG Server.....	87
To add the IP addresses of the NetScaler appliance.....	87
Verifying the NSLOG Server Configuration File.....	88
Running the NSLOG Server.....	88
To start audit server logging.....	88
To stop audit server logging that starts as a background process in FreeBSD or Linux.....	88
To stop audit server logging that starts as a service in Windows.....	88
Customizing Logging on the NSLOG Server.....	89
Creating Filters.....	89
To create a filter.....	89
Specifying Log Properties.....	90
Default Settings for the Log Properties.....	91
Sample Configuration File (audit.conf).....	92
<b>4 Web Server Logging.....</b>	<b>93</b>
Configuring the NetScaler Appliance for Web Server Logging.....	94
Enabling or Disabling Web Server Logging.....	94
To enable or disable Web server logging by using the NetScaler command line.....	94
To enable or disable Web server logging by using the configuration utility.....	95

Modifying the Default Buffer Size.....	95
To modify the buffer size by using the NetScaler command line .....	95
Parameter for modifying the buffer size.....	95
To modify the buffer size by using the configuration utility.....	96
Installing and Configuring the Client System for Web Server Logging.....	96
Installing NSWL Client on a Solaris Operating System.....	97
To install the NSWL client package on a Solaris operating system.....	97
To uninstall the NSWL client package on a Solaris operating system.....	98
Installing NSWL Client on a Linux Operating System.....	98
To install the NSWL client package on a Linux operating system.....	98
To uninstall the NSWL client package on a Linux operating system .....	99
To get more information about the NSweblog RPM file .....	99
To view the installed Web server logging files .....	99
Installing NSWL Client on a FreeBSD Operating System.....	99
To install the NSWL client package on a FreeBSD operating system.....	99
To uninstall the NSWL client package on a FreeBSD operating system.....	100
Installing NSWL Client on a Mac OS Operating System.....	100
To install the NSWL client package on a Mac OS operating system.....	100
To uninstall the NSWL client package on a Mac OS operating system.....	101
Installing NSWL Client on a Windows Operating System.....	101
To download NSWL client package from <a href="http://www.Citrix.com">www.Citrix.com</a> .....	101
To install the NSWL client on a Windows system.....	101
To uninstall the NSWL client on a Windows system.....	102
Installing NSWL Client on an AIX Operating System.....	102
To install the NSWL client package on an AIX operating system.....	102
To uninstall the NSWL client package on an AIX operating system.....	102
To get more information about the NSweblog RPM file.....	103
To view the installed Web server logging files.....	103
NSWL Client Command Options.....	103
Adding the IP Addresses of the NetScaler Appliance.....	104
To add the NSIP address of the NetScaler appliance.....	104
Verifying the NSWL Configuration File.....	105
To verify the configuration in the NSWL configuration file.....	105
Running the NSWL Client.....	105
To start Web server logging.....	105
To stop Web server logging started as a background process on the Solaris or Linux operating systems.....	105
To stop Web server logging started as a service on the Windows operating system .....	105

Customizing Logging on the NSWL Client System.....	105
Creating Filters.....	106
.....	106
To create a filter .....	107
To create a filter for a virtual server .....	107
Specifying Log Properties.....	107
Understanding the NCSA and W3C Log Formats.....	109
NCSA Common Log Format.....	109
W3C Extended Log Format.....	110
Entries.....	111
Directives.....	111
Fields.....	112
Identifiers.....	112
Creating a Custom Log Format.....	114
Creating a Custom Log Format by Using the NSWL Library.....	114
Creating a Custom Log Format Manually.....	115
Creating Apache Log Formats.....	116
Sample Configuration File.....	116
Arguments for Defining a Custom Log Format.....	118
Time Format Definition.....	121
<b>5 Advanced Configurations.....</b>	<b>125</b>
Configuring Clock Synchronization.....	126
Setting Up Clock Synchronization by Using the CLI or the Configuration Utility. ....	126
To add an NTP server by using the NetScaler command line.....	126
To modify or remove NTP servers by using the NetScaler command line.....	127
Parameters for configuring an NTP server.....	127
To configure an NTP server by using the configuration utility.....	127
Starting or Stopping the NTP Daemon.....	128
To enable or disable NTP synchronization by using the NetScaler command line.....	128
To enable or disable NTP synchronization by using the configuration utility. . .	128
Configuring Clock Synchronization Manually.....	128
To enable clock synchronization on your NetScaler by modifying the ntp.conf file.....	128
Viewing the System Date and Time.....	129
To view the system date and time by using the NetScaler command line.....	129
To view the system date and time by using the configuration utility.....	130
Configuring TCP Window Scaling.....	130

To configure window scaling by using the NetScaler command line.....	131
Parameters for configuring window scaling.....	131
To configure window scaling by using the configuration utility.....	132
Configuring Selective Acknowledgment.....	132
To enable Selective Acknowledgment (SACK) by using the NetScaler command line.....	132
To enable SACK by using the Configuration Utility.....	133
Clearing the Configuration.....	133
To clear a configuration by using the NetScaler command line.....	133
Parameters for clearing a configuration.....	134
To clear a configuration by using the configuration utility.....	134
Viewing the HTTP Band Statistics.....	134
To view HTTP request and response size statistics by using the NetScaler command line.....	134
To view HTTP request and response size statistics by using the configuration utility .....	135
To modify the band range by using the NetScaler command line.....	135
Parameters for modifying the band range for HTTP request or response size statistics.....	135
To modify the band range by using the configuration utility.....	136
Configuring HTTP Profiles.....	136
To add an HTTP profile by using the NetScaler command line.....	136
Parameters for adding an HTTP profile.....	137
To add an HTTP profile by using the configuration utility.....	138
Configuring TCP Profiles.....	138
To add a TCP profile by using the NetScaler command line.....	139
Parameters for creating a TCP profile.....	140
To add a TCP profile by using the configuration utility.....	141
Specifying a TCP Buffer Size.....	142
To set the TCP buffer size in an entity-level TCP profile by using the NetScaler command line.....	142
Example.....	143
To set the TCP buffer size in the global TCP profile by using the NetScaler command line.....	143
Example.....	143
Parameters for setting the TCP buffer size in a TCP profile.....	144
To set the TCP buffer size in a TCP profile by using the NetScaler configuration utility.....	144
Optimizing the TCP Maximum Segment Size for a Virtual Server Configuration.....	144

Specifying the MSS Value in a TCP Profile.....	145
To specify the MSS value in a TCP profile by using the NetScaler command-line.....	145
Parameters for specifying the MSS value in a TCP profile.....	145
To specify the MSS value in a TCP profile by using the NetScaler configuration utility.....	145
Configuring the NetScaler to Learn the MSS Value from Bound Services.....	146
To configure the NetScaler to learn the MSS for a virtual server by using the NetScaler command-line.....	146
Parameters for configuring the NetScaler to learn the MSS for a virtual server.....	147
To configure the NetScaler to learn the MSS for a virtual server by using the NetScaler configuration utility.....	147
<b>6 Web Interface.....</b>	<b>149</b>
How Web Interface Works.....	150
Prerequisites.....	150
Installing the Web Interface.....	151
To install the Web interface and JRE tar files by using the NetScaler command line.....	151
Parameters for installing the Web interface and JRE tar files.....	152
To install the Web interface and JRE tar files by using the configuration utility.....	152
Configuring the Web Interface.....	152
Parameters for configuring Web interface sites.....	153
Configuring a Web Interface Site for LAN Users Using HTTP.....	155
To configure a Web interface site for LAN users using HTTP by using the configuration utility.....	156
To configure a Web interface site for LAN users using HTTP by using the command line.....	158
Configuring a Web Interface Site for LAN Users Using HTTPS.....	159
To configure a Web interface site for LAN users using HTTPS by using the configuration utility.....	159
To configure a Web interface site for LAN users using HTTPS by using the command line.....	161
Configuring a Web Interface Site for Remote Users Using AGEE.....	163
To configure a Web interface site for remote users using AGEE by using the configuration utility.....	164
To configure a Web interface site for remote users using AGEE by using the command line.....	165

<b>7</b>	<b>AppFlow.....</b>	<b>167</b>
	How AppFlow Works.....	168
	Flow Records.....	169
	Templates.....	169
	Configuring the AppFlow Feature.....	170
	Enabling or Disabling the AppFlow Feature.....	171
	To enable or disable the AppFlow feature by using the NetScaler command line.....	171
	To enable the AppFlow feature by using the configuration utility.....	171
	Specifying a Collector.....	171
	To specify a collector by using the NetScaler command line.....	171
	To remove a collector by using the NetScaler command line.....	172
	Parameters for specifying a collector.....	172
	To specify a collector by using the configuration utility.....	172
	Configuring an AppFlow Action.....	172
	To configure an AppFlow action by using the NetScaler command line.....	172
	To modify or remove an AppFlow action by using the NetScaler command line.....	173
	Parameters for configuring an AppFlow action.....	173
	To configure an AppFlow action by using the configuration utility.....	174
	Configuring an AppFlow Policy.....	174
	To configure an AppFlow policy by using the NetScaler command line.....	174
	To modify or remove an AppFlow policy by using the NetScaler command line.....	175
	Parameters for configuring an AppFlow policy.....	175
	To configure an AppFlow policy by using the configuration utility.....	176
	To add an expression by using the Add Expression dialog box.....	176
	Binding an AppFlow Policy.....	177
	To globally bind an AppFlow policy by using the NetScaler command line.....	177
	To bind an AppFlow policy to a specific virtual server by using the NetScaler command line.....	178
	Parameters for binding an AppFlow policy.....	178
	To globally bind an AppFlow policy by using the configuration utility.....	178
	To bind an AppFlow policy to a specific virtual server by using the configuration utility.....	179
	Enabling AppFlow for Virtual Servers.....	179
	To enable AppFlow for a virtual server by using the NetScaler command line.....	179

---

To enable AppFlow for a virtual server by using the configuration utility. . . . .	179
Enabling AppFlow for a Service. . . . .	180
To enable AppFlow for a service by using the NetScaler command line. . . . .	180
To enable AppFlow for a service by using the configuration utility. . . . .	180
Setting the AppFlow Parameters. . . . .	180
To set the AppFlow Parameters by using the NetScaler Command Line. . . . .	180
To return AppFlow parameters to their default values by using the NetScaler command line. . . . .	181
AppFlow Parameters. . . . .	181
To set the AppFlow parameters by using the configuration utility. . . . .	182
<b>8 Reporting Tool. . . . .</b>	<b>183</b>
Using the Reporting Tool. . . . .	184
To invoke the Reporting tool. . . . .	184
Working with Reports. . . . .	184
Using Built-in Reports. . . . .	185
Creating and Deleting Reports. . . . .	185
Modifying the Time Interval. . . . .	186
Setting the Data Source and Time Zone. . . . .	187
Exporting and Importing Custom Reports. . . . .	187
Working with Charts. . . . .	188
Adding a Chart. . . . .	188
Modifying a Chart. . . . .	188
Viewing a Chart. . . . .	189
Deleting a Chart. . . . .	192
Examples. . . . .	192
To display the trend report for CPU usage and memory usage for the last week . . . . .	192
To compare the bytes received rate and the bytes transmitted rate between two interfaces for the last week. . . . .	192
Stopping and Starting the Data Collection Utility. . . . .	193
To stop nscollect. . . . .	194
To start nscollect on the local system. . . . .	194
To start nscollect on the remote system. . . . .	195
Example. . . . .	195

---

## Contents

---



---

# Preface

Learn about the Citrix® NetScaler® collection of documentation, including information about support options and ways to send us feedback.

## In This Preface:

- ◆ Formatting Conventions for NetScaler Documentation
- ◆ Documentation Available on the NetScaler Appliance
- ◆ Getting Service and Support
- ◆ NetScaler Documentation Feedback

For information about new features and enhancements for this release, see the *Citrix NetScaler 9.3 Release Notes* at <http://support.citrix.com/article/CTX128669>.

## Formatting Conventions for NetScaler Documentation

The NetScaler documentation uses the following formatting conventions.

**Table 1. Formatting Conventions**

Convention	Meaning
<b>Boldface</b>	In text paragraphs or steps in a procedure, information that you type exactly as shown (user input), or an element in the user interface.
Monospace	Text that appears in a command-line interface. Used for examples of command-line procedures. Also used to distinguish interface terms, such as names of directories and files, from ordinary text.
<angle brackets>	A term enclosed in angle brackets is a variable placeholder, to be replaced with an appropriate value. Do not enter the angle brackets.
[ brackets ]	Optional items in command statements. For example, in the following command, [ -range <positiveInteger> ] means that

Convention	Meaning
	<p>you have the option of entering a range, but it is not required:</p> <pre>add lb vserver &lt;name&gt; &lt;serviceType&gt; &lt;IPAddress&gt; &lt;port&gt; [ -range &lt;positiveInteger&gt;]</pre> <p>Do not type the brackets themselves.</p>
(vertical bar)	<p>A separator between options in braces or brackets in command statements. For example, the following indicates that you choose one of the following load balancing methods:</p> <pre>&lt;lbMethod&gt; = ( ROUNDROBIN   LEASTCONNECTION   LEASTRESPONSETIME   URLHASH   DOMAINHASH   DESTINATIONIPHASH   SOURCEIPHASH   SRCIPDESTIPHASH   LEASTBANDWIDTH   LEASTPACKETS   TOKEN   SRCIPSRCPORHASH   LRTM   CALLIDHASH   CUSTOMLOAD )</pre>
... (ellipsis)	<p>You can repeat the previous item or items in command statements. For example, <code>/route:&lt;DeviceName&gt;[ ,...]</code> means you can type additional <code>&lt;DeviceNames&gt;</code> separated by commas.</p>

## Documentation Available on the NetScaler Appliance

A complete set of Citrix® NetScaler® documentation is available on the **Documentation** tab of your NetScaler appliance and at <http://support.citrix.com/> (PDF version), and at <http://edocs.citrix.com> (HTML version). (The PDF version of the documents require Adobe Reader, available at [http://adobe.com/.](http://adobe.com/))

### To view the documentation

1. From a Web browser, log on to the NetScaler Appliance.
2. Click the **Documentation** tab.
3. To view a short description of each document, hover the mouse pointer over the title. To open a document, click the title.

## Getting Service and Support

Citrix® offers a variety of resources for support with your Citrix environment, including the following:

- ♦ The Knowledge Center is a self-service, Web-based technical support database that contains thousands of technical solutions, including access to the latest hotfixes, service packs, and security bulletins.
- ♦ Technical Support Programs for both software support and appliance maintenance are available at a variety of support levels.
- ♦ The Subscription Advantage program is a one-year membership that gives you an easy way to stay current with the latest product version upgrades and enhancements.
- ♦ Citrix Education provides official training and certification programs on virtually all Citrix products and technologies.

For more information about Citrix services and support, see the Citrix Systems Support Web site at <http://www.citrix.com/lang/English/support.asp>.

You can also participate in and follow technical discussions offered by the experts on various Citrix products at the following sites:

- ♦ <http://community.citrix.com>
- ♦ <http://twitter.com/citrixsupport>
- ♦ <http://forums.citrix.com/support>

## NetScaler Documentation Feedback

You are encouraged to provide feedback and suggestions so that we can enhance the documentation. You can send an email to [nsdocs\\_feedback@citrix.com](mailto:nsdocs_feedback@citrix.com). In the subject line, specify "Documentation Feedback." Please include the title of the guide and the page number in the email message.

You can also provide feedback through the Knowledge Center at <http://support.citrix.com/>.

### To provide feedback at the Knowledge Center home page

1. Go to the Knowledge Center home page at <http://support.citrix.com/>.
2. On the Knowledge Center home page, under **Products**, expand **NetScaler**, and then click the NetScaler release for which you want to provide feedback.
3. On the **Documentation** tab, click the guide name, and then click **Article Feedback**.
4. On the **Documentation Feedback** page, complete the form, and then click **Submit**.



---

# Chapter 1

## Authentication and Authorization

### Topics:

- [Configuring Users and Groups](#)
- [Configuring Command Policies](#)
- [Resetting the Default Administrator \(nsroot\) Password](#)
- [Example of a User Scenario](#)
- [Configuring External User Authentication](#)

To configure Citrix® NetScaler® authentication and authorization, you must first define the users who have access to the NetScaler appliance, and then you can organize these users into groups. After configuring users and groups, you need to configure command policies to define types of access, and assign the policies to users and/or groups.

You must log on as an administrator to configure users, groups, and command policies. The default NetScaler administrator user name is *nsroot*. After logging on as the default administrator, you should change the password for the *nsroot* account. Once you have changed the password, no user can access the NetScaler appliance until you create an account for that user. If you forget the administrator password after changing it from the default, you can reset it to *nsroot*.

## Configuring Users and Groups

You must define your users by configuring accounts for them. To simplify the management of user accounts, you can organize them into groups.

You can also customize the NetScaler command-line prompt for a user. Prompts can be defined in a user's configuration, in a user-group configuration, and in the global configuration. The prompt displayed for a given user is determined by the following order of precedence:

1. Display the prompt as defined in the user's configuration.
2. Display the prompt as defined in the group configuration for the user's group.
3. Display the prompt as defined in the system global configuration.

You can now specify a time-out value for inactive CLI sessions for a system user. If a user's CLI session is idle for a time that exceeds the time-out value, the NetScaler appliance terminates the connection. The timeout can be defined in a user's configuration, in a user-group configuration, and in the global configuration. The time-out for inactive CLI sessions for a user is determined by the following order of precedence:

1. Time-out value as defined in the user's configuration.
2. Time-out value as defined in the group configuration for the user's group.
3. Time-out value as defined in the system global configuration.

## Configuring User Accounts

To configure user accounts, you simply specify user names and passwords. You can change passwords and remove user accounts at any time.

### To create a user account by using the NetScaler command line

At the NetScaler command prompt, type the following command to create a user account and verify the configuration:

- ♦ **add system user** <userName> [-promptString <string>] [-timeout <secs>]
- ♦ **show system user**

#### Example

```
> add system user user1
Enter password:
Confirm password:
Done

> add system user johnd -promptString user-%u-at-%T
Enter password:
Confirm password:
Done
```

```
> show system user
1)      User name: nsroot
2)      User name: user1
3)      User name: johnd  Prompt String: user-%u-at-
%T Prompt Inherited From: User
Done
```

## To modify or remove a user account by using the NetScaler command line

- ◆ To modify a user's password, type the **set system user <userName>** command and the parameters to be changed, with their new values.
- ◆ To remove a user account, type the **rm system user <userName>** command.

## Parameters for configuring a user account

### userName (User Name)

A name for the user. The name can begin with a letter, number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (\_) symbols.

### password (Password)

A password that the user uses to log on.

### promptString (CLI Prompt)

A name for the user's NetScaler command-line prompt. The name can consist of letters, numbers, the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), underscore (\_) symbols, and the following variables:

- ◆ **%u**—Is replaced by the user name.
- ◆ **%h**—Is replaced by the host name of the NetScaler appliance.
- ◆ **%t**—Is replaced by the current time in 12-hour format.
- ◆ **%T**—Is replaced by the current time in 24-hour format.
- ◆ **%d**—Is replaced by the current date.
- ◆ **%s**—Is replaced by the state of the NetScaler appliance.

A maximum of 63 characters are allowed for this parameter. A variable (for example, %u) is counted as two characters. The resulting prompt can be longer than 63 characters.

### timeout (CLI Idle Session Timeout (Secs))

Time-out value, in seconds, for inactive CLI sessions for a system user. If a user's CLI session is idle for a time that exceeds the time-out value, the NetScaler appliance terminates the connection.

## To configure a user account by using the configuration utility

1. In the navigation pane, expand **System** and click **Users**.
2. In the details pane, do one of the following:
  - To create a user account, click **Add**.
  - To modify an existing user account, select the user, and then click **Open**.
3. In the **Create System User** or **Configure System User** dialog box, set the following parameters:
  - **User Name\***(Cannot be changed for an existing user.)
  - **Password\***
  - **Confirm Password\***
  - **CLI Prompt**
  - **CLI Idle Session Timeout (Secs)**

\* A required parameter
4. Click **Create** or **OK**, and then click **Close**.  
A message appears in the status bar, stating that the user has been configured successfully.

## Configuring User Groups

After configuring a user group, you can easily grant the same access rights to everyone in the group. To configure a group, you create the group and bind users to the group. You can bind each user account to more than one group. Binding user accounts to multiple groups may allow more flexibility when applying command policies.

### To create a user group by using the NetScaler command line

At the NetScaler command prompt, type the following commands to create a user group and verify the configuration:

- ♦ **add system group** <groupName> [-promptString <string>] [-timeout <secs>]
- ♦ **show system group**

#### Example

```
> add system group Managers -promptString Group-
Managers-at-%h
Done
> show system group
1)      Group name: group1
2)      Group name: Managers   Prompt String: Group-
Managers-at-%h
Done
```



## To modify or remove a user group by using the NetScaler command line

- ♦ To modify a user group, type the **set system group** <groupName> command and the parameters to be changed, with their new values.
- ♦ To remove a user group, type **rm system group** <groupName>.

## To bind a user to a group by using the NetScaler command line

At the NetScaler command prompt, type the following commands to bind a user account to a group and verify the configuration:

- ♦ **bind system group** <groupName> -userName <userName>
- ♦ **show system group** <groupName>

### Example

```
> bind system group Managers -userName user1
Done

> bind system group Managers -userName johnd
Done

> show system group Managers
   Group name: Managers   Prompt String: Group-
Managers-at-%h
   User name: user1
   User name: johnd
Done

> show system user user1
User name: user1   Prompt String: Group-Managers-at-
%h   Prompt Inherited From: Group

   Group name: Managers
Done

> show system user johnd
User name: johnd   Prompt String: user-%u-at-%T
Prompt Inherited From: User

   Group name: Managers
Done
```

## To unbind a user from a group by using the NetScaler command line

At the NetScaler command prompt, type the following commands to unbind a user account and verify the configuration:

- ♦ **unbind system group** <groupName> -userName <userName>
- ♦ **show system group** <groupName>

## Parameters for configuring a user group

### groupName (Group Name)

A name for the group you are creating. The name can begin with a letter, number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (\_) symbols. (Cannot be changed for existing groups.)

### userName

The name that was assigned to a previously configured user.

### promptString (CLI Prompt)

A name for the NetScaler command-line prompt for all the users that are part of this group. The name can consist of letters, numbers, the hyphen (-), period (.), pound (#), space ( ), at sign (@), equals (=), colon (:), underscore (\_) symbols, and the following variables:

- ♦ **%u**—Is replaced by the user name.
- ♦ **%h**—Is replaced by the host name of the NetScaler appliance.
- ♦ **%t**—Is replaced by the current time in 12-hour format.
- ♦ **%T**—Is replaced by the current time in 24-hour format.
- ♦ **%d**—Is replaced by the current date.
- ♦ **%s**—Is replaced by the state of the NetScaler appliance.

A maximum of 63 characters are allowed for this parameter. A variable (for example, %u) is counted as two characters. The resulting prompt can be longer than 63 characters.

### timeout (CLI Idle Session Timeout (Secs))

Time-out value, in seconds, for inactive CLI sessions for all the users that are part of this group. If a user's CLI session is idle for a time that exceeds the time-out value, the NetScaler appliance terminates the connection.

## To configure a user group by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Groups**.
2. In the details pane, do one of the following:
  - To create a new user group, click **Add**.
  - To modify an existing user group, select the group, and then click **Open**.
3. In the **Create System Group** or **Configure System Group** dialog box, set the following parameters:

- **Group Name\*** (Required for a new group. Cannot be changed for an existing group.)
- **CLI Prompt**
- **CLI Idle Session Timeout (Secs)**

\* A required parameter

4. Under **Members**, select users from the **Available Users** list and click **Add** to move them to the **Configured Users** list.
5. Click **Create** or **OK**, and then click **Close**.  
A message appears in the status bar, stating that the group has been configured successfully.

## Configuring Command Policies

Command policies regulate which commands, command groups, vservers, and other entities that users and user groups are permitted to use.

The Citrix® NetScaler® appliance provides a set of built-in command policies, and you can configure custom policies. To apply the policies, you bind them to users and/or groups.

Here are the key points to keep in mind when defining and applying command policies.

- ◆ You cannot create global command policies. Command policies must be bound directly to NetScaler users and groups.
- ◆ Users or groups with no associated command policies are subject to the default (DENY-ALL) command policy, and are therefore unable to execute any configuration commands until the proper command policies are bound to their accounts.
- ◆ All users inherit the policies of the groups to which they belong.
- ◆ You must assign a priority to a command policy when you bind it to a user account or group account. This enables the NetScaler to determine which policy has priority when two or more conflicting policies apply to the same user or group.
- ◆ The following commands are available by default to any user and are unaffected by any command you specify:  
**help cli, show cli attribute, clear cli prompt, alias, unalias, help, history, quit, exit, whoami, config, set cli mode, unset cli mode, show cli mode, set cli prompt, and show cli prompt.**

## Built-in Command Policies

The following table describes the built-in policies.

**Table 1-1. Built-in Command Policies**

Policy name	Allows
read-only	Read-only access to all <b>show</b> commands except <b>show runningconfig</b> , <b>show ns.conf</b> , and the <b>show</b> commands for the NetScaler command group.
operator	Read-only access and access to commands to enable and disable services and servers or place them in ACCESSDOWN mode.
network	Full access, except to the <b>set</b> and <b>unset</b> SSL commands, <b>sh ns.conf</b> , <b>sh runningconfig</b> , and <b>sh gslb runningconfig</b> commands.
superuser	Full access. Same privileges as the nsroot user.

## Creating Custom Command Policies

Regular expression support is offered for users with the resources to maintain more customized expressions, and for those deployments that require the flexibility that regular expressions offer. For most users, the built-in command policies are sufficient. Users who need additional levels of control but are unfamiliar with regular expressions may want to use only simple expressions, such as those in the examples provided in this section, to maintain policy readability.

When you use a regular expression to create a command policy, keep the following in mind.

- When you use regular expressions to define commands that will be affected by a command policy, you must enclose the commands in double quotation marks. For example, to create a command policy that includes all commands that begin with **show**, type the following:

```
"^show .*"
```

To create a command policy that includes all commands that begin with **rm**, type the following:

```
"^rm .*"
```

- Regular expressions used in command policies are not case sensitive.

The following table lists examples of regular expressions:

**Table 1-2. Examples of Regular Expressions for Command Policies**

Command specification	Matches these commands
"^rm\s+.*\$"	All remove actions, because all remove actions begin with the <b>rm</b> string, followed by a space and additional parameters and flags.
"^show\s+.*\$"	All show commands, because all show actions begin with the <b>show</b> string, followed by a space and additional parameters and flags.
"^shell\$"	The shell command alone, but not combined with any other parameters or flags.
"^add\s+vserver\s+.*\$"	All create vserver actions, which consist of the <b>add vserver</b> command followed by a space and additional parameters and flags.
"^add\s+(lb\s+vserver)\s+.*"	All create lb vserver actions, which consist of the <b>add lb vserver</b> command followed by a space and additional parameters and flags.

The following table shows the command specifications for each of the built-in command policies.

**Table 1-3. Expressions Used in the Built-in Command Policies**

Policy name	Command specification regular expression
read-only	(^man.*) ^show\s+(?!system)(?!ns ns.conf)(?!ns runningConfig).*) ^stat.*)
operator	(^man.*) ^show\s+(?!system)(?!ns ns.conf)(?!ns runningConfig).*) ^stat.*) ^set.*-accessdown.*) ^enable disable(server service).*)
network	^(?!shell)\S+\s+(?!system)(?!ns ns.conf)(?!ns runningConfig).*)
superuser	.*

## To create a command policy by using the NetScaler command line

At the NetScaler command prompt, type the following commands to create a command policy and verify the configuration:

- ◆ `add system cmdPolicy <policyname> <action> <cmdspeg>`
- ◆ `sh system cmdPolicy`

### Example

```
> add system cmdPolicy read_all ALLOW (^show\s+(!system) (!ns ns.conf) (!ns runningConfig).*) | (^stat.*)
Done
> sh system cmdPolicy
1) Command policy: operator
2) Command policy: read-only
3) Command policy: network
4) Command policy: superuser
5) Command policy: allow_portaladmin
6) Command policy: read_all
Done
```

## To modify or remove a command policy by using the NetScaler command line

- ◆ To modify a command policy, type the `set system cmdPolicy <PolicyName>` command and the parameters to be changed, with their new values.
- ◆ To remove a command policy, type `rm system cmdPolicy <PolicyName>`.

**Note:** The built-in command policies cannot be removed.

## Parameters for configuring a command policy

### policyname

A name for the command policy you are creating. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (\_) symbols. (Cannot be changed for existing policies.)

### action

The action the policy applies when the command specification pattern matches.  
Possible values: ALLOW, DENY

### cmdspeg

Rule (expression) that the policy uses for pattern matching.

## To configure a command policy by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Command Policies**.
2. In the details pane, do one of the following:
  - To create a command policy, click **Add**.
  - To modify an existing command policy, select the command policy, and then click **Open**.
3. In the **Create Command Policy** or **Configure Command Policy** dialog box, specify values for the parameters, which correspond to the parameters described in "Parameters for configuring a command policy" as shown:
  - Policy Name\*—policyname (Cannot be changed for an existing policy.)
  - Action—action
  - Command Spec\*—cmdspec (You can type a complete expression directly into the text area, or you can click **Add** or **Regex Tokens** for assistance. The **Add** icon opens the **Add Command** dialog box, in which you can select a NetScaler entity and then select an operation to perform on the entity. The **Regex Tokens** icon displays regular expression tokens, which you can add to your expression by selecting them.)

\* A required parameter
4. Click **Create** or **OK**, and then click **Close**.  
A message appears in the status bar, stating that the command policy has been configured successfully.

## Binding Command Policies to Users and Groups

Once you have defined your command policies, you must bind them to the appropriate user accounts and groups.

When you bind a policy, you must assign it a priority so that the NetScaler appliance can determine which command policy to follow when two or more applicable command policies are in conflict.

Command policies are evaluated in the following order:

- ♦ Command policies bound directly to users and the corresponding groups are evaluated according to priority number. A command policy with a lower priority number is evaluated before one with a higher priority number. Therefore, any privileges the lower-numbered command policy explicitly grants or denies are not overridden by a higher-numbered command policy.
- ♦ When two command policies, one bound to a user account and other to a group, have the same priority number, the command policy bound directly to the user account is evaluated first.

## To bind command policies to a user by using the NetScaler command line

At the NetScaler command prompt, type the following commands to bind a command policy to a user and verify the configuration:

- ♦ `bind system user <userName> -policyName <policyName> <priority>`
- ♦ `sh system user <userName>`

```
Example
> bind system user user1 -policyName read_all 1
Done
> sh system user user1
User name: user1
Command Policy: read_all      Priority:1
Done
```

## To unbind command policies from a user by using the NetScaler command line

At the NetScaler command prompt, type the following commands to unbind a command policy from a user and verify the configuration:

- ♦ `unbind system user <userName> -policyName <policyName>`
- ♦ `sh system user <userName>`

## Parameters for binding a command policy to a user

### userName

The name of an existing user account.

### policyName

The name of an existing command policy.

### priority

The priority assigned to this policy.

## To bind command policies to a user by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Users**.
2. In the details pane, select the user to which you want to bind a command policy, and then click **Open**.
3. In the **Configure System User** dialog box, under **Command Policies**, all of the command policies configured on your NetScaler appear on the list. Select the check box next to the name of the policy you want to bind to this user.



4. In the **Priority** column to the left, modify the default priority as needed to ensure that the policy is evaluated in the proper order.
5. Click **OK**.  
A message appears in the status bar, stating that the user has been configured successfully.

## To bind command policies to a group by using the NetScaler command line

At the NetScaler command prompt, type the following commands to bind a command policy to a user group and verify the configuration:

- ♦ **bind system group** <groupName> -policyName <policyName> <priority>
- ♦ **sh system group** <groupName>

### Example

```
> bind system group Managers -policyName read_all 1
Done
> sh system group Managers
      Group name: Managers

      User name: johnd

      Command policy: read_all          Priority:1
Done
```

## To unbind command policies from a group by using the NetScaler command line

At the NetScaler command prompt, type the following commands to unbind a command policy from a user group and verify the configuration:

- ♦ **unbind system group** <groupName> -policyName <policyName>
- ♦ **sh system group** <groupName>

## Parameters for binding a command policy to a group

### groupName

The name of an existing user group.

### policyName

The name of an existing command policy.

### priority

The priority assigned to this command policy.

## To bind command policies to a group by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Groups**.
2. In the details pane, select the group to which you want to bind a command policy, and then click **Open**.
3. In the **Configure System Group** dialog box, under **Command Policies**, all the command policies configured on your NetScaler appear on the list. Select the check box next to the name of the policy you want to bind to this group.
4. In the **Priority** column to the left, modify the default priority as needed to ensure that the policy is evaluated in the proper order.
5. Click **OK**.  
A message appears in the status bar, stating that the group has been configured successfully.

## Resetting the Default Administrator (nsroot) Password

The nsroot account provides complete access to all features of the Citrix® NetScaler® appliance. Therefore, to preserve security, the nsroot account should be used only when necessary, and only individuals whose duties require full access should know the password for the nsroot account. Frequently changing the nsroot password is advisable. If you lose the password, you can reset it to the default and then change it.

To reset the nsroot password, you must boot the NetScaler into single user mode, mount the file systems in read/write mode, and remove the set NetScaler user nsroot entry from the ns.conf file. You can then reboot, log on with the default password, and choose a new password.

### To reset the nsroot password

1. Connect a computer to the NetScaler serial port and log on.

**Note:** You cannot log on by using ssh to perform this procedure; you must connect directly to the NetScaler appliance.

As the operating system starts, it displays the following message:

```
Hit [Enter] to boot immediately, or any other key for  
command prompt.
```

```
Booting [kernel] in # seconds.
```

2. Press CTRL+C.  
The following message appears:

Type '?' for a list of commands, 'help' for more detailed help.

ok

3. Type **boot -s** and press the ENTER key to start the NetScaler in single user mode.

After the NetScaler boots, it displays the following message:

Enter full path name of shell or RETURN for /bin/sh:

4. Press the ENTER key to display the # prompt, and type the following commands to mount the file systems:

```
fsck /dev/ad0s1a
```

```
mount /dev/ad0s1a /flash
```

5. Using a text editor of your choice, edit the /flash/nsconfig/ns.conf file and remove the set system user nsroot entry.
6. Save the file and exit the text editor.
7. Type **reboot** and press the ENTER key to reboot the NetScaler.  
When the NetScaler completes rebooting, it prompts for the user name and password.
8. Log on with the nsroot user credentials.  
Once logged on to the NetScaler, you will be required to enter a new nsroot user password.
9. Follow the prompts to change the password.
10. Exit the **config ns** menu.

## Example of a User Scenario

The following example shows how to create a complete set of user accounts, groups, and command policies and bind each policy to the appropriate groups and users. The company, Example Manufacturing, Inc., has three users who can access the Citrix® NetScaler® appliance:

- ♦ **John Doe.** The IT manager. John needs to be able to see all parts of the NetScaler configuration but does not need to modify anything.
- ♦ **Maria Ramiez.** The lead IT administrator. Maria needs to be able to see and modify all parts of the NetScaler configuration except for NetScaler commands (which local policy dictates must be performed while logged on as nsroot).
- ♦ **Michael Baldrock.** The IT administrator in charge of load balancing. Michael needs to be able to see all parts of the NetScaler configuration, but needs to modify only the load balancing functions.

The following table shows the breakdown of network information, user account names, group names, and command policies for the sample company.

**Table 1-4. Sample Values for Creating Entities**

Field	Value	Note
NetScaler host name	ns01.example.net	N/A
User accounts	johnd, mariar, and michaelb	John Doe, IT manager, Maria Ramirez, IT administrator and Michael Baldrick, IT administrator.
Groups	Managers and SysOps	All managers and all IT administrators.
Command Policies	read_all, modify_lb, and modify_all	Allow complete read-only access, Allow modify access to load balancing, and Allow complete modify access.

The following description walks you through the process of creating a complete set of user accounts, groups, and command policies on the NetScaler appliance named ns01.example.net.

The description includes procedures for binding the appropriate user accounts and groups to one another, and binding appropriate command policies to the user accounts and groups.

This example illustrates how you can use prioritization to grant precise access and privileges to each user in the IT department.

The example assumes that initial installation and configuration have already been performed on the NetScaler.

## Configuration steps

1. Use the procedure described in [Configuring User Accounts](#) on page 22 to create user accounts **johnd**, **mariar**, and **michaelb**.
2. Use the procedure described in [Configuring User Groups](#) on page 24 to create user groups **Managers** and **SysOps**, and then bind the users **mariar** and **michaelb** to the **SysOps** group and the user **johnd** to the **Managers** group.
3. Use the procedure described in [Creating Custom Command Policies](#) on page 28 to create the following command policies:
  - **read\_all** with action **Allow** and command spec "(^show\s+(?!system)(?!ns ns.conf)(?!ns runningConfig).\*)|(^stat.\*)"
  - **modify\_lb** with action as **Allow** and the command spec "^set\s+lb\s+.\*\$"
  - **modify\_all** with action as **Allow** and the command spec "^S\s+(?!system).\*"

4. Use the procedure described in [Binding Command Policies to Users and Groups](#) on page 31 to bind the `read_all` command policy to the `SysOps` group, with priority value 1.
5. Use the procedure described in [Binding Command Policies to Users and Groups](#) on page 31 to bind the `modify_lb` command policy to user `michaelb`, with priority value 5.

The configuration you just created results in the following:

- ♦ John Doe, the IT manager, has read-only access to the entire NetScaler configuration, but he cannot make modifications.
- ♦ Maria Ramirez, the IT lead, has near-complete access to all areas of the NetScaler configuration, having to log on only to perform NetScaler-level commands.
- ♦ Michael Baldrock, the IT administrator responsible for load balancing, has read-only access to the NetScaler configuration, and can modify the configuration options for load balancing.

The set of command policies that applies to a specific user is a combination of command policies applied directly to the user's account and command policies applied to the group(s) of which the user is a member.

Each time a user enters a command, the operating system searches the command policies for that user until it finds a policy with an ALLOW or DENY action that matches the command. When it finds a match, the operating system stops its command policy search and allows or denies access to the command.

If the operating system finds no matching command policy, it denies the user access to the command, in accordance with the NetScaler appliance's default deny policy.

**Note:** When placing a user into multiple groups, take care not to cause unintended user command restrictions or privileges. To avoid these conflicts, when organizing your users in groups, bear in mind the NetScaler command policy search procedure and policy ordering rules.

## Configuring External User Authentication

External user authentication is the process of authenticating the users of the Citrix® NetScaler® appliance by using an external authentication server. The NetScaler supports LDAP, RADIUS, TACACS+, and NT4 authentication servers. To configure external user authentication, you must create authentication policies. You can configure one or many authentication policies, depending on your authentication needs. An authentication policy consists of an expression and an action. Authentication policies use NetScaler classic expressions, which are described in detail in the *Citrix NetScaler Policy Configuration and Reference Guide* at <http://support.citrix.com/article/CTX128673>.

After creating an authentication policy, you bind it to the system global entity and assign a priority to it. You can create simple server configurations by binding a single authentication policy to the system global entity. Or, you can configure a cascade of authentication servers by binding multiple policies to the system global entity. If no

authentication policies are bound to the system, users are authenticated by the onboard system.

**Note:** User accounts must be configured on the NetScaler appliance before users can be externally authenticated. You must first create an onboard system user for all users who will access the appliance, so that you can bind command policies to the user accounts. Regardless of the authentication source, users cannot log on if they are not granted sufficient command authorization through command policies bound to their user accounts or to a group of which they are a member.

## Configuring LDAP Authentication

You can configure the NetScaler to authenticate user access with one or more LDAP servers. LDAP authorization requires identical group names in Active Directory, on the LDAP server, and on the NetScaler. The characters and case must also be the same.

By default, LDAP authentication is secured by using SSL/TLS protocol. There are two types of secure LDAP connections. In the first type, the LDAP server accepts the SSL/TLS connection on a port separate from the port used to accept clear LDAP connections. After users establish the SSL/TLS connection, LDAP traffic can be sent over the connection. The second type allows both unsecured and secure LDAP connections and is handled by a single port on the server. In this scenario, to create a secure connection, the client first establishes a clear LDAP connection. Then the LDAP command StartTLS is sent to the server over the connection. If the LDAP server supports StartTLS, the connection is converted to a secure LDAP connection by using TLS.

The port numbers for LDAP connections are:

- ◆ 389 for unsecured LDAP connections
- ◆ 636 for secure LDAP connections
- ◆ 3268 for Microsoft unsecure LDAP connections
- ◆ 3269 for Microsoft secure LDAP connections

LDAP connections that use the StartTLS command use port number 389. If port numbers 389 or 3268 are configured on the NetScaler, it tries to use StartTLS to make the connection. If any other port number is used, connection attempts use SSL/TLS. If StartTLS or SSL/TLS cannot be used, the connection fails.

When configuring the LDAP server, the case of the alphabetic characters must match that on the server and on the NetScaler. If the root directory of the LDAP server is specified, all of the subdirectories are also searched to find the user attribute. In large directories, this can affect performance. For this reason, Citrix recommends that you use a specific organizational unit (OU).

The following table lists examples of user attribute fields for LDAP servers.

**Table 1-5. User Attribute Fields for LDAP Servers**

LDAP server	User attribute	Case sensitive?
Microsoft Active Directory	Server sAMAccountName	No
Novell eDirectory	cn	Yes
IBM Directory Server	uid	Yes
Lotus Domino	CN	Yes
Sun ONE directory (formerly iPlanet)	uid or cn	Yes

The following table lists examples of the base distinguished name (DN).

**Table 1-6. Examples of Base Distinguished Name**

LDAP server	Base DN
Microsoft Active Directory	DC=citrix, DC=local
Novell eDirectory	dc=citrix, dc=net
IBM Directory Server	cn=users
Lotus Domino	OU=City, O=Citrix, C=US
Sun ONE directory (formerly iPlanet)	ou=People, dc=citrix, dc=com

The following table lists examples of the bind distinguished name (DN).

**Table 1-7. Examples of Bind Distinguished Name**

LDAP server	Bind DN
Microsoft Active Directory	CN=Administrator, CN=Users, DC=citrix, DC=local
Novell eDirectory	cn=admin, dc=citrix, dc=net
IBM Directory Server	LDAP_dn

LDAP server	Bind DN
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE directory (formerly iPlanet)	uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot

## To configure LDAP authentication by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Authentication**.
2. On the **Policies** tab, click **Add**.
3. In **Name**, type a name for the policy.
4. In **Authentication Type**, select **LDAP**. Next to **Server**, click **New**.
5. In **Name**, type the name of the server.
6. Under **Server**, in **IP Address** and **Port**, type the IP address and port number of the LDAP server.
7. Under **Connection Settings**, provide the following information:

- In **Base DN (location of users)**, type the base DN under which users are located.

Base DN is usually derived from the Bind DN by removing the user name and specifying the group where in which are located. Examples of syntax for base DN are:

```
ou=users, dc=ace, dc=com
cn=Users, dc=ace, dc=com
```

- In **Administrator Bind DN**, type the administrator bind DN for queries to the LDAP directory. Examples for syntax of bind DN are:

```
domain/user name
ou=administrator, dc=ace, dc=com
user@domain.name (for Active Directory)
cn=Administrator, cn=Users, dc=ace, dc=com
```

For Active Directory, the group name specified as `cn=groupname` is required. The group name that is defined in the NetScaler must be identical to the group name that is defined on the LDAP server. For other LDAP directories, the group name either is not required or, if required, is specified as `ou=groupname`.

The NetScaler binds to the LDAP server, using the administrator credentials, and then searches for the user. After locating the user, the NetScaler unbinds the administrator credentials and rebinds with the user credentials.

- In **Administrator Password** and **Confirm Administrator Password**, type the administrator password for the LDAP server.



8. To retrieve additional LDAP settings automatically, click **Retrieve Attributes**. The fields under **Other Settings** then populate automatically. If you do not want to do this, skip to Step 12.
9. Under **Other Settings**, in **Server Logon Name Attribute**, type the attribute under which the NetScaler should look for user logon names for the LDAP server that you are configuring. The default is `samAccountName`.
10. In **Group Attribute**, leave the default `memberOf` for Active Directory or change it to that of the LDAP server type you are using. This attribute enables the NetScaler to obtain the groups associated with a user during authorization.
11. In **Security Type**, select the security type.  
If you select **PLAINTEXT** or **TLS** for security, use port number 389. If you select **SSL**, use port number 636.
12. To allow users to change their LDAP password, select **Allow Password Change**.  
If you select **PLAINTEXT** as the security type, allowing users to change their passwords is not supported.
13. Click **Create**.
14. In the **Create Authentication Policy** dialog box, next to **Named Expressions**, select the expression, click **Add Expression**, click **Create**, and click **Close**.

After the LDAP server settings are configured on the NetScaler, bind the policy to the system global entity. For more information about binding authentication policies globally, see [Binding the Authentication Policies to the System Global Entity](#) on page 45.

## Determining attributes in the LDAP directory

If you need help determining your LDAP directory attributes, you can easily look them up with the free LDAP browser from Softerra.

You can download the LDAP browser from the Softerra LDAP Administrator Web site at <http://www.ldapbrowser.com>. After the browser is installed, set the following attributes:

- ◆ The host name or IP address of your LDAP server.
- ◆ The port of your LDAP server. The default is 389.
- ◆ The base DN field can be left blank.
- ◆ The information provided by the LDAP browser can help you determine the base DN needed for the Authentication tab.
- ◆ The Anonymous Bind check determines whether the LDAP server requires user credentials for the browser to connect to it. If the LDAP server requires credentials, leave the check box cleared.

After completing the settings, the LDAP browser displays the profile name in the left pane and connects to the LDAP server.

## Configuring RADIUS Authentication

You can configure the NetScaler appliance to authenticate user access with one or more RADIUS servers. If you are using RSA SecurID, SafeWord, or Gemalto Protiva products, use a RADIUS server.

Your configuration might require using a network access server IP address (NAS IP) or a network access server identifier (NAS ID). When configuring your NetScaler to use a RADIUS authentication server, use the following guidelines:

- ◆ If you enable use of the NAS IP, the appliance sends its configured IP address to the RADIUS server, rather than the source IP address used in establishing the RADIUS connection.
- ◆ If you configure the NAS ID, the appliance sends the identifier to the RADIUS server. If you do not configure the NAS ID, the appliance sends its host name to the RADIUS server.
- ◆ When the NAS IP is enabled, the appliance ignores any NAS ID that was configured by using the NAS IP to communicate with the RADIUS server.

### To configure RADIUS authentication by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Authentication**.
2. On the **Policies** tab, click **Add**.
3. In **Name**, type a name for the policy.
4. In **Authentication Type**, select **RADIUS**.
5. Next to **Server**, click **New**.
6. In **Name**, type a name for the server.
7. Under **Server**, in **IP Address**, type the IP address of the RADIUS server.
8. In **Port**, type the port. The default is 1812.
9. Under **Details**, in **Secret Key** and **Confirm Secret Key**, type the RADIUS server secret.
10. In **NAS ID**, type the identifier number, and then click **Create**.
11. In the **Create Authentication Policy** dialog box, next to **Named Expressions**, select the expression, click **Add Expression**, click **Create**, and click **Close**.

After the RADIUS server settings are configured on the NetScaler, bind the policy to the system global entity. For more information about binding authentication policies globally, see [Binding the Authentication Policies to the System Global Entity](#) on page 45.

### Choosing RADIUS authentication protocols

The NetScaler appliance supports implementations of RADIUS that are configured to use any of several protocols for user authentication, including:

- ◆ Password Authentication Protocol
- ◆ Challenge-Handshake Authentication Protocol (CHAP)
- ◆ Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP Version 1 and Version 2)

If your deployment of the NetScaler is configured to use RADIUS authentication and your RADIUS server is configured to use Password Authentication Protocol, you can strengthen user authentication by assigning a strong shared secret to the RADIUS server. Strong RADIUS shared secrets consist of random sequences of uppercase and lowercase letters, numbers, and punctuation, and are at least 22 characters long. If possible, use a random character generation program to determine RADIUS shared secrets.

To further protect RADIUS traffic, assign a different shared secret to each NetScaler appliance or virtual server. When you define clients on the RADIUS server, you can also assign a separate shared secret to each client. If you do this, you must configure separately each NetScaler policy that uses RADIUS authentication.

Shared secrets are configured on the NetScaler when a RADIUS policy is created.

## Configuring IP address extraction

You can configure the NetScaler to extract the IP address from a RADIUS server. When a user authenticates with the RADIUS server, the server returns a framed IP address that is assigned to the user. The following are attributes for IP address extraction:

- ◆ Allows a remote RADIUS server to supply an IP address from the internal network for a user logged on to the NetScaler.
- ◆ Allows configuration for any RADIUS attribute using the type `ipaddress`, including those that are vendor encoded.

When configuring the RADIUS server for IP address extraction, you configure the vendor identifier and the attribute type.

The vendor identifier enables the RADIUS server to assign an IP address to the client from a pool of IP addresses that are configured on the RADIUS server. The vendor ID and attributes are used to make the association between the RADIUS client and the RADIUS server. The vendor ID is the attribute in the RADIUS response that provides the IP address of the internal network. A value of zero indicates that the attribute is not vendor encoded. The attribute type is the remote IP address attribute in a RADIUS response. The minimum value is one and the maximum value is 255.

A common configuration is to extract the RADIUS attribute *framed IP address*. The vendor ID is set to zero or is not specified. The attribute type is set to eight.

### To configure IP address extraction by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Authentication**.
2. On the **Policies** tab, click **Open**.
3. In the **Configure Authentication Policy** dialog box, next to **Server**, click **Modify**.
4. Under **Details**, in **Group Vendor Identifier**, type the value.

5. In **Group Attribute Type**, type the value, and click **OK** twice.

## Configuring TACACS+ Authentication

You can configure a TACACS+ server for authentication. Similar to RADIUS authentication, TACACS+ uses a secret key, an IP address, and the port number. The default port number is 49. To configure the NetScaler to use a TACACS+ server, provide the server IP address and the TACACS+ secret. The port needs to be specified only when the server port number in use is something other than the default port number of 49.

### To configure TACACS+ authentication by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Authentication**.
2. On the **Policies** tab, click **Add**.
3. In **Name**, type a name for the policy.
4. In **Authentication Type**, select **TACACS**.
5. Next to **Server**, click **New**.
6. In **Name**, type a name for the server.
7. Under **Server**, type the IP address and port number of the TACACS+ server.
8. Under **TACACS server information**, in **TACACS Key** and **Confirm TACACS key**, type the key.
9. In **Authorization**, select **ON** and click **Create**.
10. In the **Create Authentication Policy** dialog box, next to **Named Expressions**, select the expression, click **Add Expression**, click **Create**, and click **Close**.

After the TACACS+ server settings are configured on the NetScaler, bind the policy to the system global entity. For more information about binding authentication policies globally, see [Binding the Authentication Policies to the System Global Entity](#) on page 45.

## Configuring NT4 Authentication

You can configure the NetScaler appliance to use Windows NT LAN Manager (NTLM) authentication to authenticate users against the user database on a Windows NT 4.0 domain controller. A Windows NT 4.0 domain controller maintains domain user accounts in a database on the Windows NT 4.0 server. A domain user account includes a user name and password and other information about the user.

When a user logs on to the NetScaler, the user enters the user name and password maintained in the domain user account on the Windows NT 4.0 server. The NetScaler connects to the Windows NT 4.0 server and passes these credentials to the server. The server authenticates the user. If you need to configure the NetScaler to authenticate clients against a Windows NT 4.0 primary or backup domain controller, you need to specify the server IP address, the domain name, and the domain administrator user

name and password of the person who is authorized to administer the domain. These parameters are necessary because the NetScaler joins the domain to communicate authentication data.

NT4 authentication supports NTLMv1 and NTLMv2 authentication protocols only.

### **To configure NT4 authentication by using the configuration utility**

1. In the navigation pane, expand **System**, and then click **Authentication**.
2. On the **Policies** tab, click **Add**.
3. In **Name**, type a name for the policy.
4. In **Authentication Type**, select **NT4**.
5. Next to **Server**, click **New**.
6. In **Server**, type the name of the server.
7. Complete the settings as they are configured on your Windows NT 4.0 server and click **Create**.
8. In the **Create Authentication Policy** dialog box, next to **Named Expressions**, select the expression, click **Add Expression**, click **Create**, and click **Close**.

When the settings for Windows NT 4.0 authentication are configured, bind the policy to the system global entity. For more information about binding authentication policies globally, see [Binding the Authentication Policies to the System Global Entity](#) on page 45.

## **Binding the Authentication Policies to the System Global Entity**

When the authentication policies are configured, bind the policies to the system global entity.

### **To bind an authentication policy globally by using the configuration utility**

1. In the navigation pane, expand **System**, and then click **Authentication**.
2. On the **Policies** tab, click **Global Bindings**.
3. Under **Details**, click **Insert Policy**.
4. Under **Policy Name**, select the policy and click **OK**.

### **To unbind a global authentication policy by using the configuration utility**

1. In the navigation pane, expand **System**, and then click **Authentication**.

2. On the **Policies** tab, click **Global Bindings**.
3. In the **Bind/Unbind Authentication Policies** dialog box, in **Policy Name**, select the policy, click **Unbind Policy** and then click **OK**.

## Chapter 2

# SNMP

### Topics:

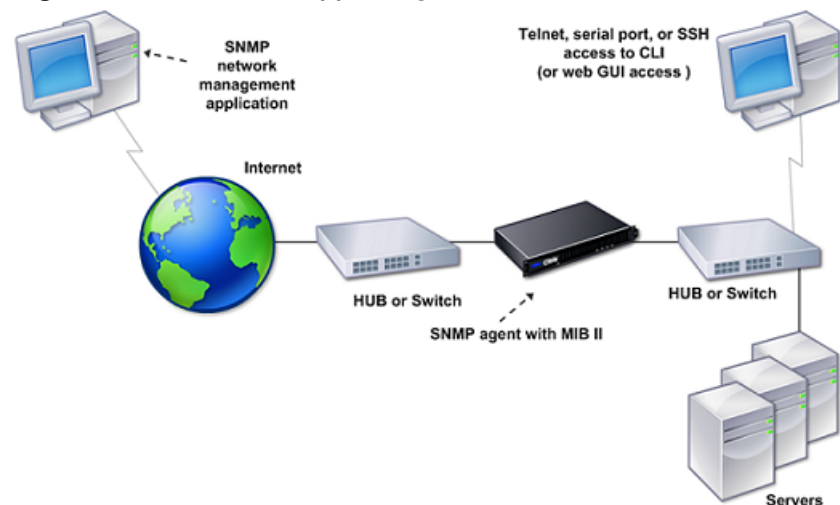
- [Importing MIB Files to the SNMP Manager and Trap Listener](#)
- [Configuring the NetScaler to Generate SNMPv1 and SNMPv2 Traps](#)
- [Configuring the NetScaler for SNMP v1 and v2 Queries](#)
- [Configuring SNMP Alarms for Rate Limiting](#)
- [Configuring the NetScaler for SNMPv3 Queries](#)

You can use Simple Network Management Protocol (SNMP) to configure the SNMP agent on the Citrix® NetScaler® appliance to generate asynchronous events, which are called *traps*. The traps are generated whenever there are abnormal conditions on the NetScaler. The traps are then sent to a remote device called a *trap listener*, which signals the abnormal condition on the NetScaler appliance. Or, you can query the SNMP agent for System-specific information from a remote device called an *SNMP manager*. The agent then searches the management information base (MIB) for the data requested and sends the data to the SNMP manager.

The SNMP agent on the NetScaler can generate traps compliant with SNMPv1 and SNMPv2 only. For querying, the SNMP agent supports SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2), and SNMP version 3 (SNMPv3).

The following figure illustrates a network with a NetScaler that has SNMP enabled and configured. In the figure, each SNMP network management application uses SNMP to communicate with the SNMP agent on the NetScaler. The SNMP agent searches its management information base (MIB) to collect the data requested by the SNMP Manager and provides the information to the application.

**Figure 2-1. NetScaler Supporting SNMP**



## Importing MIB Files to the SNMP Manager and Trap Listener

You must download the following files to SNMP managers and trap listeners before you start monitoring a NetScaler appliance.

- ♦ **NS-MIB-smiv1.mib.** This file is used by SNMPv1 managers and trap listeners.
- ♦ **NS-MIB-smiv2.mib.** This file is used by SNMPv2 and SNMPv3 managers and SNMPv2 trap listeners.

The MIB files include the following:

- ♦ **A subset of standard MIB-2 groups.** Provides the MIB-2 groups SYSTEM, IF, ICMP, UDP, and SNMP.
- ♦ **A NetScaler enterprise MIB.** Provides NetScaler-specific configuration and statistics.

### To import the MIB files to the SNMP manager and trap listener

- ♦ Logon to the **Downloads** page of NetScaler appliance GUI.
- ♦ Under **SNMP Files**, do one of the following:
  - a. If your SNMP management application is other than WhatsUpGold, download the following files to your SNMP management application:
    - ♦ NS-MIB-smiv2.mib
    - ♦ NS-MIB-smiv1.mib
  - b. If you are using the WhatsUpGold SNMP management application, download only the following files to the SNMP management application:
    - ♦ mib.txt
    - ♦ traps.txt

## Configuring the NetScaler to Generate SNMPv1 and SNMPv2 Traps

You can configure the NetScaler to generate asynchronous events, which are called *traps*. The traps are generated whenever there are abnormal conditions on the NetScaler. The traps are sent to a remote device called a *trap listener*. This helps administrators monitor the NetScaler and respond promptly to any issues.

The NetScaler provides a set of condition entities called *SNMP alarms*. When the condition in any SNMP alarm is met, the NetScaler generates SNMP trap messages that



are sent to the configured trap listeners. For example, when the LOGIN-FAILURE alarm is enabled, a trap message is generated and sent to the trap listener whenever there is a login failure on the NetScaler appliance.

To configure the NetScaler to generate traps, you need to enable and configure alarms. Then, you specify trap listeners to which the NetScaler will send the generated trap messages.

## Enabling or Disabling an SNMP Alarm

The NetScaler generates traps only for SNMP alarms that are enabled. Some alarms are enabled by default, but you can disable them.

When you enable an SNMP alarm, the NetScaler generates corresponding trap messages when some events occur. Some NetScaler alarms are enabled by default.

### To enable or disable an SNMP alarm by using the command line

At the NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ◆ `enable snmp alarm <alarm name>`
- ◆ `sh snmp alarm <alarm name>`

#### Example

```
> enable snmp alarm LOGIN-FAILURE
Done
> show snmp alarm LOGIN-FAILURE
Alarm Alarm Threshold Normal Threshold Time State
Severity Logging
-----
1) LOGIN-FAILURE N/A N/A N/A ENABLED - ENABLED
Done
```

### To enable or disable an SNMP alarm by using the configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Alarms**.
2. In the details pane, select an alarm (for example, **Login-Failure**), and do one of the following:
  - To enable an alarm, click **Enable**.
  - To disable an alarm, click **Disable**.

A message appears in the status bar, stating that the alarm is enabled or disabled successfully.

## Configuring Alarms

The NetScaler provides a set of condition entities called *SNMP alarms*. When the condition set for an SNMP alarm is met, the NetScaler generates SNMP traps messages that are sent to the configured trap listeners. For example, when the LOGIN-FAILURE alarm is enabled, a trap message is generated and sent to the trap listener whenever there is a login failure on the NetScaler appliance.

You can assign an SNMP alarm with a severity level. When you do this, the corresponding trap messages are assigned that severity level.

The following are the severity levels, defined in the NetScaler, in decreasing order of severity.

- ♦ Critical
- ♦ Major
- ♦ Minor
- ♦ Warning
- ♦ Informational

For example, if you set a Warning severity level for the SNMP alarm named LOGIN-FAILURE, the trap messages generated when there is a login failure will be assigned with the Warning severity level.

You can also configure an SNMP alarm to log the corresponding trap messages generated whenever the condition on that alarm is met.

### To configure an SNMP alarm by using the command line

At the NetScaler command prompt, type the following commands to configure an SNMP alarm and verify the configuration:

- ♦ **set snmp alarm** <alarm Name> [-thresholdValue <positive\_integer> [-normalValue <positive\_integer>]] [-time <secs>] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]
- ♦ **sh snmp alarm** <alarm Name>

### Parameters for configuring SNMP alarms

#### severity

Severity level of this alarm. Possible values: Critical, Major, Minor, Warning, Informational. Default: Informational.

#### logging

Enable logging of SNMP trap messages by Syslog. Possible values: ENABLED and DISABLED.

## To configure SNMP alarms by using the configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Alarms**.
2. In the details pane, select an alarm (for example, **Login-Failure**), and then click **Open**.
3. In the **Configure SNMP Alarm** dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring SNMP alarms" as shown:
  - **Severity**—severity
  - **Logging**—logging
4. Click **OK**.

A message appears in the status bar, stating that the alarm has been configured successfully.

## Configuring Traps

After configuring the alarms, you need to specify the trap listener to which the NetScaler appliance sends the trap messages. Apart from specifying parameters such as IP address and the destination port of the trap listener, you can specify the type of trap (either generic or specific) and the SNMP version.

You can configure a maximum of 20 trap listeners for receiving either generic or specific traps.

You can also configure the NetScaler to send SNMP trap messages with a source IP, other than the NetScaler IP address (NSIP), to a particular trap listener. You can set the source IP to either a mapped IP address (MIP) or a subnet IP address (SNIP) configured on the NetScaler appliance.

You can also configure the NetScaler to send trap messages to a trap listener on the basis of a severity level. For example, if you set the severity level as Minor for a trap listener, all trap messages of the severity level equal to or greater than Minor (Minor, Major, and Critical) are sent to the trap listener.

If you have defined a community string for the trap listener, you must also specify a community string for each trap that is to be sent to the listener. A trap listener for which a community string has been defined accepts only trap messages that include a community string matching the community string defined in the trap listener. Other trap messages are dropped.

## To add an SNMP trap by using the NetScaler command line

At the NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ♦ **add snmp trap** <trapClass> <trapDestination> -version ( V1 | V2 ) -destPort <port> -communityName <string> -srcIP <ip\_addr> -severity <severity>

## ♦ show snmp trap

```

Example
add snmp trap specific 10.102.29.3 -version V2 -
destPort 80 -communityName com1 -severity Major
Done
> show snmp trap
Type          DestinationIP      DestinationPort
Version       SourceIP          Min-Severity
Community
-----
-----
-----
generic       10.102.29.9      162
V2            NetScaler IP     N/A              public
specific      10.102.29.9      162
V2            NetScaler IP     -                public
specific      10.102.29.3      80
V2            NetScaler IP     Major            com1
Done

```

**Parameters for configuring SNMP traps****trapClass**

The trap type. Possible values: generic and specific.

**version**

SNMP version of the trap PDU to be sent.

**trapDestination**

IPv4 address of the trap listener.

**destPort**

Destination port of the trap. Default: 162. Minimum value: 1

**scrIP**

Source IP of the traps.

**severity**

Specify the severity level of trap messages. All generated trap messages of the severity level up to the specified severity level will be sent to the trap listener.

Possible values: Critical, Major, Minor, Warning, and Informational.

Default: Informational.

**communityName**

The community string. Default: public.

**To configure SNMP Traps by using the configuration utility**

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Traps**.

2. In the details pane, do one of the following:
  - To create a new trap, click **Add**.
  - To modify an existing trap, select the trap, and then click **Open**.
3. In the **Create SNMP Trap Destination** or **Configure SNMP Trap** dialog box, set the following parameters:
  - **Type\***—trapClass
  - **Version**—version
  - **Destination IP Address\***—trapDestination
  - **Destination Port**—destPort
  - **Source IP Address**—srcIP
  - **Minimum Severity**—severity
  - **Community Name**—communityName

\*A required parameter
4. Click **Create** or **OK**, and then click **Close**.  
A message appears in the status bar, stating that the trap has been configured successfully.

## Enabling Unconditional SNMP Trap Logging

By default, the NetScaler appliance logs any SNMP trap messages (for SNMP alarms in which logging is enabled) when at least one trap listener is specified on the NetScaler appliance. However, you can specify that SNMP trap messages be logged even when no trap listeners are configured.

### To enable or disable unconditional SNMP trap logging by using the NetScaler command line

At a NetScaler command prompt, type:

- ♦ **set snmp option -snmpTrapLogging ( ENABLED | DISABLED )**
- ♦ **show snmp option**

#### Example

```
> set snmp option -snmpset ENABLED
Done
> show snmp option
      Snmpset:  DISABLED      SnmpTrapLogging:
ENABLED
Done
>
```

## Parameters for unconditional SNMP trap logging

### SnmpTrapLogging (SNMP Trap Logging)

Enable the NetScaler appliance to log any SNMP traps messages (for those respective SNMP alarms in which logging is enabled) even when no trap listeners are configured. Possible Values: ENABLED, DISABLED. Default: DISABLED.

## To enable or disable unconditional SNMP trap logging by using the configuration utility

1. In the navigation pane, expand **System**, and then click **SNMP**.
2. In the details pane, under **Settings**, click **Configure SNMP Options**.
3. In the **Configure SNMP Options** dialog box, select the **SNMP Trap Logging** check box.
4. Click **OK**.

# Configuring the NetScaler for SNMP v1 and v2 Queries

You can query the NetScaler SNMP agent for system-specific information from a remote device called *SNMP managers*. The agent then searches the management information base (MIB) for the data requested and sends the data to the SNMP manager.

The following types of SNMP v1 and v2 queries are supported by the SNMP agent:

- ◆ GET
- ◆ GET NEXT
- ◆ ALL
- ◆ GET BULK

You can create strings called *community strings* and associate each of these to query types. You can associate one or more community strings to each query type. Community string are passwords and used to authenticate SNMP queries from SNMP managers.

For example, if you associate two community strings, such as **abc** and **bcd**, to the query type GET NEXT, the SNMP agent on the NetScaler appliance considers only those GET NEXT SNMP query packets that contain **abc** or **bcd** as the community string.

## Specifying an SNMP Manager

You must configure the NetScaler appliance to allow the appropriate SNMP managers to query it. You must also provide the SNMP manager with the required NetScaler-specific information. You can add up to a maximum of 100 SNMP managers or networks.

For an IPv4 SNMP manager you can specify a host name instead of the manager's IP address. If you do so, you must add a DNS name server that resolves the host name of

the SNMP manager to its IP address. You can add up to a maximum of five host-name based SNMP managers.

If you do not configure at least one SNMP manager, the NetScaler appliance accepts and responds to SNMP queries from all IP addresses on the network. If you configure one or more SNMP managers, the appliance accepts and responds only to SNMP queries from those specific IP addresses.

If you remove an SNMP manager from the NetScaler configuration, that manager can no longer query the NetScaler.

## To add an SNMP manager by using the NetScaler command line

At the NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ◆ **add snmp manager** <IPAddress> ... [-netmask <netmask>]
- ◆ **show snmp manager**

### Example

```
> add snmp manager 10.102.29.10
Done
> show snmp manager
1)      10.102.29.5          255.255.255.255
Done
```

## To add an SNMP manager by specifying its IP address, using the NetScaler command line

At the NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ◆ **add snmp manager** <IPAddress> ... [-netmask <netmask>]
- ◆ **show snmp manager**

### Example

```
> add snmp manager 10.102.29.10
Done
> show snmp manager
1)      10.102.29.5          255.255.255.0
Done

> add snmp manager 10.102.29.15 10.102.29.30
Done
> show snmp manager
1)      IP Address:         10.102.29.10
        Netmask:           255.255.255.255
2)      IP Address:         10.102.29.15
        Netmask:           255.255.255.255
3)      IP Address:         10.102.29.30
```

```

Netmask:          255.255.255.255
Done

```

## To add an SNMP manager by specifying its host name, using the NetScaler command line

**Important:** If you specify the SNMP manager's host name instead of its IP address, you must configure a DNS name server to resolve the host name to the SNMP manager's IP address. For more information, see the instructions for adding a name server in the *Citrix NetScaler Traffic Management Guide*. For a link to the guide, see the [Documentation Library](#).

At the NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ◆ **add snmp manager** <IPAddress> [-domainResolveRetry <integer>]
- ◆ **show snmp manager**

```

Example
> add nameserver 10.103.128.15
Done
> show nameserver
1)      10.103.128.15  -  State: UP
Done

> add snmp manager engwiki.eng.example.net -
domainResolveRetry 10
Done
> show snmp manager
1)      Hostname:      abc.com (Unresolved IP)
        Resolve Retry: 7
2)      Hostname:      engwiki.eng.example.net
        (10.217.3.249)
        Resolve Retry: 10
Done

```

## Parameters for configuring an SNMP manager

### IPAddress

Can be any of the following:

- ◆ IPv4 address of the SNMP manager.
- ◆ IPv4 network address. The NetScaler appliance accepts and responds to SNMP queries from any device on this network.
- ◆ Associated host name of an SNMP manager that has an IPv4 address. If you specify a host name, you must add a DNS name server that resolves the host name of the SNMP manager to its IP address.



**Note:** The NetScaler appliance does not support host names for SNMP managers that have IPv6 addresses.

**netmask**

Subnet of management stations. Used to grant access from entire subnets to the NetScaler appliance.

**domainResolveRetry**

The duration, in seconds, for which the NetScaler appliance waits to send the next DNS query to resolve the host name of the SNMP manager if the last query failed. If last query succeeds, the NetScaler waits for the TTL time. Minimum value: 5. Maximum value: 20940. Default value: 5.

## To add an SNMP manager by using the configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Managers**.
  2. In the details pane, click **Add**.
  3. In the **Create SNMP Manager** dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring an SNMP manager" as shown:
    - **IP Address\***—IPAddress
    - **Netmask**—netmask
    - \*A required parameter
  4. In the **Create SNMP Manager** dialog box, do one of the following:
    - To specify the host name of an SNMP manager, select **Management Host** and set the following parameters:
      - ♦ **Host Name\***—IPAddress
      - ♦ **Resolve Retry (secs)\***—domainResolveRetry
- Important:** If you specify the SNMP manager's host name instead of its IPv4 address, you must configure a DNS name server to resolve the host name to the SNMP manager's IP address. For more information, see the instructions for adding a name server in the *Citrix NetScaler Traffic Management Guide*. For a link to the guide, see the [Documentation Library](#).
- To specify the IPv4 address of an SNMP manager, select **Management Network** and set the following parameters:
    - ♦ **IP Address\***—IPAddress
    - ♦ **Netmask**—netmask
  5. Click **Create**, and then click **Close**.  
A message appears in the status bar, stating that the SNMP manager has been configured successfully.

## Specifying an SNMP Community

You can create strings called *community strings* and associate them with the following SNMP query types on the NetScaler:

- ♦ GET
- ♦ GET NEXT
- ♦ ALL
- ♦ GET BULK

You can associate one or more community strings to each query types. For example, when you associate two community strings, such as `abc` and `bcd`, to the query type GET NEXT, the SNMP agent on the NetScaler appliance considers only those GET NEXT SNMP query packets that contain `abc` or `bcd` as the community string.

If you don't associate any community string to a query type then the SNMP agent responds to all SNMP queries of that type.

### To specify an SNMP community by using the NetScaler command line

At the NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ♦ `add snmp community <communityName> <permissions>`
- ♦ `sh snmp community`

#### Example

```
> add snmp community com all
Done
> show snmp community com
Community: com Permissions: ALL
Done
```

### Parameters for configuring an SNMP community string

#### **communityName**

SNMP community string.

#### **permissions**

Access privileges. Possible values: GET, GET NEXT, GET BULK, ALL.

### To configure an SNMP community string by using the configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Community**.

2. In the details pane, click **Add**.
3. In the **Create SNMP Community** dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring an SNMP community string" as shown:
  - **Community String\***—communityName
  - **Permission\***—permissions

\*A required parameter
4. Click **Create**, and then click **Close**.

A message appears in the status bar, stating that the SNMP community string has been configured successfully.

### To remove an SNMP community string by using the configuration utility

1. In the navigation pane, expand **System**, click **SNMP**, and then click **Community**.
2. In the details pane, select the community that you want to remove (for example, **Com\_All**), and then click **Remove**.

## Configuring SNMP Alarms for Rate Limiting

Citrix® NetScaler® appliances such as the NetScaler MPX 10500, 12500, and 15500 are rate limited. The maximum throughput (Mbps) and packets per second (PPS) are determined by the license purchased for the appliance. For rate-limited platforms, you can configure SNMP traps to send notifications when throughput and PPS approach their limits and when they return to normal.

Throughput and PPS are monitored every seven seconds. You can configure traps with high-threshold and normal-threshold values, which are expressed as a percentage of the licensed limits. The appliance then generates a trap when throughput or PPS exceeds the high threshold, and a second trap when the monitored parameter falls to the normal threshold. In addition to sending the traps to the configured destination device, the NetScaler logs the events associated with the traps in the `/var/log/ns.log` file as `EVENT ALERTSTARTED` and `EVENT ALERTENDED`.

Exceeding the throughput limit can result in packet loss. You can configure SNMP alarms to report packet loss.

For more information about SNMP alarms and traps, see [Configuring the NetScaler to Generate SNMPv1 and SNMPv2 Traps](#) on page 48.

## Configuring an SNMP Alarm for Throughput or PPS

To monitor both throughput and PPS, you must configure separate alarms.

## To configure an SNMP alarm for the throughput rate by using the NetScaler command line

At the NetScaler command prompt, type the following commands to configure the SNMP alarm and verify the configuration:

- ◆ **set snmp alarm PF-RL-RATE-THRESHOLD** [-thresholdValue <positive\_integer> [-normalValue <positive\_integer>]] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]
- ◆ **show snmp alarm PF-RL-RATE-THRESHOLD**

```

Example
> set snmp alarm PF-RL-RATE-THRESHOLD -
thresholdValue 70 -normalValue 50
Done

> show snmp alarm PF-RL-RATE-THRESHOLD
Alarm Alarm Threshold
Normal Threshold Time State Severity
Logging
-----
-----
1) PF-RL-RATE-THRESHOLD 70
50 N/A DISABLED -
ENABLED
Done

```

## To modify or remove the threshold values by using the NetScaler command line

- ◆ To modify the threshold values, type the **set snmp alarm PF-RL-RATE-THRESHOLD** command and the parameters to be changed, with their new values.
- ◆ To remove the threshold values, type the **unset snmp alarm PF-RL-RATE-THRESHOLD** command, followed by the **-thresholdValue** parameter, but do not specify any value for the parameter.

**Note:** The normal-threshold value is automatically unset when you unset the high-threshold value.

## To configure an SNMP alarm for PPS by using the NetScaler command line

At the NetScaler command prompt, type the following commands to configure the SNMP alarm for PPS and verify the configuration:

- ◆ **set snmp alarm PF-RL-PPS-THRESHOLD** [-thresholdValue <positive\_integer> [-normalValue <positive\_integer>]] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]

◆ **show snmp alarm PF-RL-PPS-THRESHOLD**

```

Example
> set snmp alarm PF-RL-PPS-THRESHOLD -
thresholdValue 70 -normalValue 50
Done

> show snmp alarm PF-RL-PPS-THRESHOLD

Alarm
-----
Threshold      Alarm Threshold      Normal
Severity       Time Logging          State
-----
1) PF-RL-PPS-THRESHOLD
70
50
N/A
ENABLED
-----
Done

```

### To modify or remove the threshold values by using the NetScaler command line

- ◆ To modify the threshold values, type the **set snmp alarm PF-RL-PPS-THRESHOLD** command and the parameters to be changed, with their new values.
- ◆ To remove the threshold values, type the **unset snmp alarm PF-RL-PPS-THRESHOLD** command, followed by the **-thresholdValue** parameter, but do not specify any value for the parameter.

**Note:** The normal-threshold value is automatically unset when you unset the high-threshold value.

### Parameters for configuring an SNMP alarm for throughput or PPS

**thresholdValue**

The high threshold value, which triggers EVENT ALERTSTARTED. Minimum value: 1.

**normalValue**

The normal threshold value, which triggers EVENT ALERTENDED.

**state**

The current state of the alarm. Possible values: ENABLED, DISABLED. Default: ENABLED.

**severity**

The severity level of the alarm. Possible values: Critical, Major, Minor, Warning, Informational. Default: SNMP\_SEV\_UNKNOWN.

**logging**

Log the alarm. Possible values: ENABLED, DISABLED. Default value: ENABLED.

**To configure an SNMP alarm for throughput or PPS by using the configuration utility**

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Alarms**.
2. In the details pane, do one of the following:
  - Select **PF-RL-RATE-THRESHOLD** to configure the SNMP alarm for throughput rate.
  - Select **PF-RL-PPS-THRESHOLD** to configure the SNMP alarm for packets per second.
3. Click **Open**.
4. In the **Configure SNMP Alarm** dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring an SNMP alarm for throughput or PPS” as shown:
  - **Alarm Threshold**—thresholdValue
  - **Alarm Threshold**—thresholdValue
  - **Normal Threshold**—normalValue
  - **Severity**—severity
  - **Logging**—logging
5. Select the **Enable** check box to enable the alarm.
6. Click **OK**, and then click **Close**.

## Configuring SNMP Alarm for Dropped Packets

You can configure an alarm for packets dropped as a result of exceeding the throughput limit and an alarm for packets dropped as a result of exceeding the PPS limit.

**To configure an SNMP alarm for packets dropped because of excessive throughput, by using the NetScaler command line**

At the NetScaler command prompt, type:

```
set snmp alarm PF-RL-RATE-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-severity <severity>] [-logging ( ENABLED | DISABLED )]
```

**To configure an SNMP alarm for packets dropped because of excessive PPS, by using the NetScaler command line**

At the NetScaler command prompt, type:

```
set snmp alarm PF-RL-PPS-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-severity <severity>] [-logging ( ENABLED | DISABLED )]
```

## Parameters for configuring an SNMP alarm for dropped packets

### state

The current state of the alarm. Possible values: ENABLED, DISABLED. Default: ENABLED.

### severity

The severity level of the alarm. Possible values: Critical, Major, Minor, Warning, Informational. Default: SNMP\_SEV\_UNKNOWN.

### logging

Log the alarm. Possible values: ENABLED, DISABLED. Default value: ENABLED.

## To configure an SNMP alarm for dropped packets by using the configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Alarms**.
2. In the details pane, do one of the following:
  - Select **PF-RL-RATE-PKTS-DROPPED** to configure an SNMP alarm for packets dropped because of excessive throughput.
  - Select **PF-RL-PPS-PKTS-DROPPED** to configure an SNMP alarm for packets dropped because of excessive PPS.
3. Click **Open**.
4. In the Configure SNMP Alarm dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring an SNMP alarm for dropped packets” as shown:
  - **Severity**—severity
  - **Logging**—logging
5. Select the **Enable** check box to enable the alarm.
6. Click **OK**, and then click **Close**.

## Configuring the NetScaler for SNMPv3 Queries

Simple Network Management Protocol Version 3 (SNMPv3) is based on the basic structure and architecture of SNMPv1 and SNMPv2. However, SNMPv3 enhances the basic architecture to incorporate administration and security capabilities, such as authentication, access control, data integrity check, data origin verification, message timeliness check, and data confidentiality.

To implement message level security and access control, SNMPv3 introduces the user-based security model (USM) and the view-based access control model (VACM).

- ♦ **User-Based Security Model.** The user-based security model (USM) provides message-level security. It enables you to configure users and security parameters for the SNMP agent and the SNMP manager. USM offers the following features:

- **Data integrity:** To protect messages from being modified during transmission through the network.
- **Data origin verification:** To authenticate the user who sent the message request.
- **Message timeliness:** To protect against message delays or replays.
- **Data confidentiality:** To protect the content of messages from being disclosed to unauthorized entities or individuals.
- ♦ **View-Based Access Control Model.** The view-based access control model (VACM) enables you to configure access rights to a specific subtree of the MIB based on various parameters, such as security level, security model, user name, and view type. It enables you to configure agents to provide different levels of access to the MIB to different managers.

The Citrix NetScaler supports the following entities that enable you to implement the security features of SNMPv3:

- ♦ SNMP Engines
- ♦ SNMP Views
- ♦ SNMP Groups
- ♦ SNMP Users

These entities function together to implement the SNMPv3 security features. Views are created to allow access to subtrees of the MIB. Then, groups are created with the required security level and access to the defined views. Finally, users are created and assigned to the groups.

**Note:** The view, group, and user configuration are synchronized and propagated to the secondary node in a high availability (HA) pair. However, the engine ID is neither propagated nor synchronized as it is unique to each NetScaler appliance.

To implement message authentication and access control, you need to:

- ♦ Set the Engine ID
- ♦ Configure Views
- ♦ Configure Groups
- ♦ Configure Users

## Setting the Engine ID

SNMP engines are service providers that reside in the SNMP agent. They provide services such as sending, receiving, and authenticating messages. SNMP engines are uniquely identified using engine IDs.

The NetScaler has a unique engineID based on the MAC address of one of its interfaces. It is not necessary to override the engineID. However, if you want to change the engine ID, you can reset it.



## To set the engine ID by using the NetScaler command line

At a NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ◆ `set snmp engineId <engineID>`
- ◆ `show snmp engineId`

### Example

```
> set snmp engineId 8000173f0300c095f80c68
Done
> show snmp engineId
EngineID: 8000173f0300c095f80c68
Done
```

## Parameters for setting the engine ID

### EngineID

Engine ID of the SNMP agent.

## To set the engine ID by using configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Users**.
2. In the details pane, click **Configure Engine ID**.
3. In the **Configure Engine ID** dialog box, in the **Engine ID** text box, type an engine ID (for example, 8000173f0300c095f80c68).
4. Click **OK**.  
A message appears in the status bar, stating that the engine ID has been modified successfully.

## Configuring a View

SNMP views restrict user access to specific portions of the MIB. SNMP views are used to implement access control.

## To add an SNMP view by using the NetScaler command line

At a NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ◆ `add snmp view <name> <subtree> -type ( included | excluded )`
- ◆ `sh snmp view <name>`

### Example

```
add snmp view View1 -type included
```

## Parameters for configuring an SNMP view

**name**

Name of the SNMP view.

**subtree**

Subtree of the MIB.

**type**

Whether the subtree needs to be included or excluded.

## To configure an SNMP view by using the configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Views**.
2. In the details pane, click **Add**.
3. In the **Create SNMP View** or **Configure SNMP View** dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring an SNMP view" as shown:
  - **Name\***—name
  - **Subtree\***—subtree
  - **Type**—type

\*A required parameter
4. Click **Create** or **OK**, and then click **Close**.  
A message appears in the status bar, stating that the SNMP view has been configured successfully.

## Configuring a Group

SNMP groups are logical aggregations of SNMP users. They are used to implement access control and to define the security levels. You can configure an SNMP group to set access rights for users assigned to that group, thereby restricting the users to specific views.

You need to configure an SNMP group to set access rights for users assigned to that group.

## To add an SNMP group by using the NetScaler command line

At a NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ♦ **add snmp group** <name> <securityLevel> -readViewName <string>
- ♦ **show snmp group** <name> <securityLevel>

**Example**

```
add snmp group edocs_group2 authPriv -readViewName
edocs_read_view
Done
> show snmp group edocs_group2 authPriv
```

```

1)      Name:  edocs_group2      SecurityLevel:
authPriv
      ReadViewName:  edocs_read_view
StorageType:  volatile
      Status:  active
Done

```

## Parameters for configuring an SNMP group

### name

Name of the SNMP view.

### securityLevel

The security level of the group. Possible values: noAuthNoPriv, authNoPriv, authPriv

### readViewName

SNMP view to be associated with this group.

## To configure an SNMP group by using the configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Groups**.
2. In the details pane, click **Add**.
3. In the **Create SNMP Group** or **Configure SNMP Group** dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring an SNMP group" as shown:
  - **Name\***—name
  - **Security Level\***—securityLevel
  - **Read View Name\***—readViewName

\*A required parameter
4. Click **Create** or **OK**, and then click **Close**.  
A message appears in the status bar, stating that the SNMP group has been configured successfully.

## Configuring a User

SNMP users are the SNMP managers that the agents allow to access the MIBs. Each SNMP user is assigned to an SNMP group.

You need to configure users at the agent and assign each user to a group.

### To configure a user by using the NetScaler command line

At a NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ♦ **add snmp user <name> -group <string> [-authType ( MD5 | SHA ) {-authPasswd } [-privType ( DES | AES ) {-privPasswd }]]**

- ◆ **show snmp user <name>**

**Example**

```
> add snmp user edocs_user -group edocs_group
Done
> show snmp user edocs_user
1)      Name:  edocs_user           Group:
edocs_group
      EngineID:  123abc456abc788 StorageType:
volatile
      Status:  active
Done
>
```

## Parameters for configuring an SNMP user

**name**

The name of the SNMP user.

**group**

Specifies the SNMP group name to which the SNMP user will belong.

**authType**

The authentication type. Possible values: MD5, SHA.

**authPasswd**

Enter an authentication password.

**privType**

The encryption type. Possible values: DES, AES.

**privPasswd**

The encryption password. Maximum Length: 31

## To configure an SNMP user by using the configuration utility

1. In the navigation pane, expand **System**, expand **SNMP**, and then click **Users**.
2. In the details pane, click **Add**.
3. In the **Create SNMP User** or **Configure SNMP User** dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring an SNMP user" as shown:
  - **Name\***—name
  - **Group Name\***—group
  - **Authentication Type**—authType
  - **Authentication Password**—authPasswd
  - **Privacy Type**—privType
  - **Privacy password**—privPasswd

\*A required parameter

4. Click **Create** or **OK**, and then click **Close**.  
A message appears in the status bar, stating that the SNMP user has been configured successfully.



---

## Chapter 3

# Audit Logging

### Topics:

- [Configuring the NetScaler Appliance for Audit Logging](#)
- [Installing and Configuring the NSLOG Server](#)
- [Running the NSLOG Server](#)
- [Customizing Logging on the NSLOG Server](#)
- [Default Settings for the Log Properties](#)
- [Sample Configuration File \(audit.conf\)](#)

Auditing is a methodical examination or review of a condition or situation. The Audit Logging feature enables you to log the Citrix® NetScaler® states and status information collected by various modules in the kernel and in the user-level daemons. For audit logging, you have the options to configure SYSLOG, the native NSLOG protocol, or both.

SYSLOG is a standard protocol for logging. It has two components— the SYSLOG auditing module, which runs on the NetScaler appliance, and the SYSLOG server, which can run on the underlying FreeBSD operating system (OS) of the NetScaler appliance or on a remote system. SYSLOG uses user data protocol (UDP) for the transfer of data.

Similarly, the native NSLOG protocol has two components— the NSLOG auditing module, which runs on the NetScaler appliance, and the NSLOG server, which can run on the underlying FreeBSD OS of the NetScaler appliance or on a remote system. NSLOG uses transmission control protocol (TCP) for transfer of data.

When you run NSLOG or a SYSLOG server, it connects to the NetScaler appliance. The NetScaler appliance then starts sending all the log information to the SYSLOG or NSLOG server, and the server can filter the log entries before storing them in a log file. An NSLOG or SYSLOG server can receive log information from more than one NetScaler appliance and a NetScaler appliance can send log information to more than one SYSLOG server or NSLOG server.

The log information that a SYSLOG or NSLOG server collects from a NetScaler appliance is stored in a log file in the form of messages. These messages typically contain the following information:

- ◆ The IP address of a NetScaler appliance that generated the log message
- ◆ A time stamp
- ◆ The message type
- ◆ The predefined log levels (Critical, Error, Notice, Warning, Informational, Debug, Alert, and Emergency)
- ◆ The message information

To configure audit logging, you first configure the audit modules on the NetScaler that involves creating audit policies and specifying the NSLOG server or SYSLOG server information. You then install and configure the SYSLOG or the NSLOG server on the underlying FreeBSD OS of the NetScaler appliance or on a remote system.

**Note:** Because SYSLOG is an industry standard for logging program messages and because various vendors provide support, this documentation does not include SYSLOG server configuration information.

The NSLOG server has its own configuration file (`auditlog.conf`). You can customize logging on the NSLOG server system by making additional modifications to the configuration file (`auditlog.conf`).



# Configuring the NetScaler Appliance for Audit Logging

Policies define the SYSLOG or NSLOG protocol, and server actions define what logs are sent where. For server actions, you specify the system information, which runs the SYSLOG or the NSLOG server.

The Citrix NetScaler logs the following information related to TCP connections:

- ◆ Source port
- ◆ Destination port
- ◆ Source IP
- ◆ Destination IP
- ◆ Number of bytes transmitted and received
- ◆ Time period for which the connection is open

**Note:** You can enable TCP logging on individual load balancing vserver. You must bind the audit log policy to a specific load balancing vserver that you want to log.

## Configuring Audit Servers

You can configure audit server actions for different servers and for different log levels.

### To configure a SYSLOG server action by using the command line

At the NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ◆ **add audit syslogAction** <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
- ◆ **show audit syslogAction** [<name>]

#### Example

```
> add audit syslogaction audit-action1 10.102.1.1 -
loglevel INFORMATIONAL -dateformat MMDDYYYY
Done
> show audit syslogaction audit-action1
1)      Name: audit-action1
        Server IP: 10.102.1.1   Port: 514
        Loglevel : INFORMATIONAL
        Date Format: MMDDYYYY
        Time Zone: GMT_TIME
        Facility: LOCAL0
        Tcp Logging: NONE
        ACL Logging: DISABLED
```

```
UserDefinedLogging: No
AppFlow export: DISABLED
Done
```

## To configure an NSLOG server action by using the command line

At the NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ◆ **add audit nslogAction** <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
- ◆ **show audit nslogAction** [<name>]

### Example

```
> add audit nslogAction nslog-action1 10.102.1.3 -
serverport 520 -loglevel INFORMATIONAL -dateFormat
MMDDYYYY
Done
> show nslogAction nslog-action1
1) Name: nslog-action1
Server IP: 10.102.1.3 Port: 520
Loglevel : INFORMATIONAL
Date Format: MMDDYYYY
Time Zone: GMT_TIME
Facility: LOCAL0
Tcp Logging: NONE
ACL Logging: DISABLED
UserDefinedLogging: No
AppFlow export: DISABLED
Done
```

## Parameters for configuring auditing servers

### name

The name of the SYSLOG server action or NSLOG server action.

### serverIP

IP address of the auditing server.

### serverPort

Port through which to communicate.

### logLevel

Severity levels of messages to be logged. Possible values: ALL, NONE, or one or more of the following:

- ◆ EMERGENCY
- ◆ ALERT
- ◆ CRITICAL

- ◆ ERROR
- ◆ WARNING
- ◆ NOTICE
- ◆ INFORMATION
- ◆ DEBUG

**dateFormat**

Format of the date stamp. Possible values: MMDDYYYY, DDMMYYYY.

**logFacility**

The Facility value (RFC 3164) assigned to the log message. Uses numerical codes 0 to 7 to indicate the type of message originating from the NetScaler (for example, NS and VPN). Possible values: LOCAL0 to LOCAL7. Default: LOCAL0.

**timeZone**

Time zone for the time stamp. Possible values: GMT and Local. Default: Local.

**tcp**

Log TCP events. Possible values: NONE, ALL.

**acl**

Log ACL events. Possible values: ENABLED, DISABLED.

**userDefinedAuditlog**

Enable user-configurable log messages. Possible values: YES, NO.

**appflowExport**

Export log messages to the AppFlow collectors. Possible values: ENABLED, DISABLED. Default: DISABLED.

## Log levels defined

**EMERGENCY**

Log errors indicating that the NetScaler is experiencing a critical problem that may make it unusable.

**ALERT**

Log problems that are not critical to current operations but that indicate a need for immediate corrective action to prevent a critical problem.

**CRITICAL**

Log critical conditions, which do not restrict current operations but may escalate to a larger problem.

**ERROR**

Log messages related to failed NetScaler operations.

**WARNING**

Log issues that may result in critical errors.

**NOTICE**

Log events specified by the INFORMATION setting, but in greater detail.

#### INFORMATION

Log actions taken by the NetScaler. This level is useful for troubleshooting problems.

#### DEBUG

Log extensive, detailed information to help developers troubleshoot problems.

### To configure an auditing server action

1. In the navigation pane, expand **System**, expand **Auditing**, and then click **Policies**.
2. In the details pane, on the **Servers** tab, do one of the following:
  - To create a new server action, click **Add**.
  - To modify an existing server action, select the server, and then click **Open**.
3. In the **Create Auditing Server** or **Configure Auditing Server** dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring auditing servers" as shown:
  - **Name\***—name
  - **IP Address\***—serverIP
  - **Port**—serverPort
  - **Log Levels**—logLevel
  - **Log Facility**—logFacility
  - **Date format**—dateFormat
  - **Time Zone**—timeZone
  - **TCP Logging**—tcp
  - **ACL Logging**—acl
  - **User Configurable Log Messages**—userDefinedAuditlog
  - **AppFlow Export**—appflowExport

\*A required parameter
4. Click **Create** or **OK**, and then click **Close**.  
A message appears in the status bar, stating that the auditing server has been configured successfully.

## Configuring Audit Policies

The audit policies define the SYSLOG or NSLOG protocol.

### To configure a SYSLOG policy by using the command line

At the NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ◆ **add audit syslogPolicy** <name> <rule> <action>
- ◆ **show audit syslogPolicy** [<name>]

**Example**

```
> add audit syslogpolicy syslog-poll ns_true audit-
action1
Done
> show audit syslogpolicy syslog-poll
1)      Name: syslog-poll      Rule: ns_true
        Action: audit-action1
Done
```

**To configure an NSLOG policy by using the command line**

At the NetScaler command prompt, type the following commands to set the parameters and verify the configuration:

- ◆ **add audit nslogPolicy** <name> <rule> <action>
- ◆ **show audit nslogPolicy** [<name>]

**Example**

```
> add audit nslogPolicy nslog-poll ns_true nslog-
action1
Done
> show audit nslogPolicy nslog-poll
1)      Name: nslog-poll      Rule: ns_true
        Action: nslog-action1
Done
```

**Parameters for configuring audit policies****name**

The name of NSLOG policy or SYSLOG policy.

**rule**

The name of the rule or expression that the policy will use. It currently supports only the rule "ns\_true."

This parameter is only for the command line.

In the configuration utility ns\_true is internally assigned as a rule for the SYSLOG or the NSLOG policy.

**action**

SYSLOG server action or the NSLOG server action. NSLOG server action is bind to a NSLOG audit policy and SYSLOG server action is bind to a SYSLOG audit policy.

## To configure an audit server policy

1. In the navigation pane, expand **System**, expand **Auditing**, and then click **Policies**.
2. In the details pane, on the **Policies** tab, do one of the following:
  - To create a new policy, click **Add**.
  - To modify an existing policy, select the policy, and then click **Open**.
3. In the **Create Auditing Policy** or **Configure Auditing Policy** dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring auditing policies" as shown:
  - **Name\*** □ name
  - **Server\*** □ action

\*A required parameter
4. Click **Create** or **OK**, and then click **Close**.  
A message appears in the status bar, stating that the auditing policy has been configured successfully.

## Binding the Audit Policies Globally

You must globally bind the audit log policies to enable logging of all Citrix® NetScaler® system events. By defining the priority level, you can set the evaluation order of the audit server logging. Priority 0 is the highest and is evaluated first. The higher the priority number, the lower is the priority of evaluation.

### To configure a SYSLOG policy by using the command line

- ♦ `bind system global [<policyName> [-priority <positive_integer>]]`
- ♦ `sh system global`

#### Example

```
> bind system global nslog-poll1 -priority 20
Done

> sh system global
1) Policy Name: nslog-poll1 Priority: 20
2) Policy Name: syslog-poll1 Priority: 50
3) Policy Name: nslogpol9 Priority: 100
Done
```

### Parameters for binding the audit policies globally

#### policyName

The name of the NSLOG or SYSLOG policy.

**priority**

A numeric value that indicates when this policy is evaluated relative to others. A lower priority is evaluated before a higher one.

**To globally bind the audit policy**

1. In the navigation pane, expand **System**, expand **Auditing**, and then click **Policies**.
2. In the details pane, on the **Policies** tab, click **Global Bindings**.
3. In the **Bind/Unbind Auditing Global Policies** dialog box, click **Insert Policy**.
4. Select the policy from the drop-down list that appears under **Policy Name**, and then click **OK**.  
A message appears in the status bar, stating that the auditing policy has been globally bound.

## Configuring Policy-Based Logging

You can configure policy-based logging for rewrite and responder policies. Audit messages are then logged in a defined format when the rule in a policy evaluates to TRUE. To configure policy-based logging, you configure an audit-message action that uses default syntax expressions to specify the format of the audit messages, and associate the action with a policy. The policy can be bound either globally or to a load balancing or content switching virtual server. You can use audit-message actions to log messages at various log levels, either in syslog format only or in both syslog and newslog formats.

### Pre Requisites

- ◆ User Configurable Log Messages (userDefinedAuditlog) option is enabled for when configuring the audit action server to which you want to send the logs in a defined format. For more information about enabling policy-based logging on a audit action server, see [Binding the Audit Policies Globally](#) on page 78.
- ◆ The related audit policy is bound to system global. For more information about binding audit policies to system global, see [Binding the Audit Policies Globally](#) on page 78.

### Configuring an Audit Message Action

You can configure audit message actions to log messages at various log levels, either in syslog format only or in both syslog and newslog formats. Audit-message actions use expressions to specify the format of the audit messages.

#### To create an audit message action by using the NetScaler command line

At the NetScaler command prompt, type:

```
add audit messageaction <name> <logLevel> <stringBuilderExpr> [-logtoNewslog (YES|NO)] [-bypassSafetyCheck (YES|NO)]
```

## To modify or remove an audit message action by using the NetScaler command line

- ◆ To modify an audit message action, type the **set audit messageaction** command, the name of the action, and the parameters to be changed, with their new values.
- ◆ To remove an audit message action, type the **rm audit messageaction** command and the name of the action.

### Example

```
> add audit messageaction log-act1 CRITICAL
'"Client:"+CLIENT.IP.SRC+" accessed "+H
TTP.REQ.URL' -bypassSafetyCheck YES
Done

> show audit messageaction log-act1

1)      Name: log-act1
        LogMsgStr: "Client:"+CLIENT.IP.SRC+"
accessed "+HTTP.REQ.URL
        Loglevel:CRITICAL
        Log2Newslog:NO
        BypassSafetyCheck : YES
        Hits: 0
        Undef Hits: 0
        Action Reference Count: 0

Done
```

## Parameters for configuring an audit message action

### name

The name of the audit message action. The name can begin with a letter, number, or the underscore symbol, and can consist of up to 127 characters including letters, numbers, and hyphen (-), period (.) pound (#), space ( ), at sign (@), equal sign (=), colon (:), and underscore (\_) symbols.

### logLevel

The log level for the message action. Possible values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG, NONE.

### stringBuilderExpr

The expression that defines the format of the log message. For a complete description of NetScaler expressions, see the *Citrix NetScaler Policy Configuration and Reference Guide*. For a link to the guide, see the [Documentation Library](#).

### bypassSafetyCheck

Bypass the safety check and allow unsafe expressions. Possible values: YES, NO. Default: NO.

### logtoNewslog

Log messages in newslog format in addition to logging them in syslog format. Possible values: YES, NO. Default: NO.



## To configure an audit message action by using the configuration utility

1. In the navigation pane, expand **System**, expand **Auditing**, and then click **Message Actions**.
2. In the details pane, do one of the following:
  - To create a new audit message action, click **Add**.
  - To modify an existing audit message action, select the action, and then click **Open**.
3. In the **Create Message Action** or **Configure Message Action** dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for configuring an audit message action" as shown:
  - **Name\***—name
  - **Log Level\***—logLevel
  - **Log Message**—stringBuilderExpr
  - **Bypass Safety Check**—bypassSafetyCheck (To specify **YES**, select the check box.)
  - **Log in newnslog**—logtoNewnslog (To specify **YES**, select the check box.)

\*A required parameter
4. Click **Create** or **OK**, and then click **Close**. The audit message action that you configured appears in the details pane.

## Binding Audit Message Action to a Policy

After you have created an audit message action, you must bind it to a rewrite or responder policy. For more information about binding log message actions to a rewrite or responder policy, see the "Rewrite" or the "Responder" chapter of the *Citrix NetScaler Application Security Guide*. For a link to the guide, see the [Documentation Library](#).

# Installing and Configuring the NSLOG Server

During installation, the NSLOG server executable file (auditserver) is installed along with other files. The auditserver executable file includes options for performing several actions on the NSLOG server, including running and stopping the NSLOG server. In addition, you use the auditserver executable to configure the NSLOG server with the IP addresses of the NetScaler appliances from which the NSLOG server will start collecting logs. Configuration settings are applied in the NSLOG server configuration file (auditlog.conf).

Then, you start the NSLOG server by executing the auditserver executable. The NSLOG server configuration is based on the settings in the configuration file. You can further customize logging on the NSLOG server system by making additional modifications to the NSLOG server configuration file (auditlog.conf).

The following table lists the operating systems on which the NSLOG server is supported.

**Table 3-1. Supported Platforms for the NSLOG Server**

Operating system	Software requirements
Windows	<ul style="list-style-type: none"> <li>◆ Windows XP Professional</li> <li>◆ Windows Server 2003</li> <li>◆ Windows 2000/NT</li> </ul>
Linux	<ul style="list-style-type: none"> <li>◆ Red Hat Enterprise Linux AS release 4 (Nahant) - Linux version 2.6.9-5.EL</li> <li>◆ Red Hat 3.4.3-9.EL4 - Linux version 2.6.9-5.ELsmp</li> <li>◆ Red Hat Linux 3.2.2-5 - Linux version 2.4.20-8</li> </ul>
FreeBSD	FreeBSD 4.9

The minimum hardware specifications for the platform running the NSLOG server are as follows:

- ◆ Processor- Intel x86 ~501 megahertz (MHz)
- ◆ RAM - 512 megabytes (MB)
- ◆ Controller - SCSI

## Installing NSLOG Server on the Linux Operating System

Copy the installation files from the NetScaler product CD or download them from [ftp.netscaler.com](http://ftp.netscaler.com). Log on to the Linux system as an administrator. Use the following procedure to install the NSLOG server executable files on the system.

### To install the NSLOG server package on a Linux operating system

1. At a Linux command prompt, type the following command to copy the `NSauditserver.rpm` file to a temporary directory:

```
cp <path_to_cd>/Utilities/auditserver/Linux/NSauditserver.rpm /tmp
```

2. Type the following command to install the `NSauditserver.rpm` file:

```
rpm -i NSauditserver.rpm
```

This command extracts the files and installs them in the following directories:

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

## To uninstall the NSLOG server package on a Linux operating system

1. At a command prompt, type the following command to uninstall the audit server logging feature:

```
rpm -e NSauditserver
```

2. For more information about the NSauditserver RPM file, use the following command:

```
rpm -qpi *.rpm
```

3. To view the installed audit server files use the following command:

```
rpm -qpl *.rpm
```

\*.rpm: Specifies the file name.

## Installing NSLOG Server on the FreeBSD Operating System

Before you can install the NSLOG server, you have to copy the NSLOG package from the NetScaler product CD or download it from [www.citrix.com](http://www.citrix.com). The NSLOG package has the following name format `AuditServer_<release number>-<build number>.zip` (for example, `AuditServer_9.3-51.5.zip`). This package contains NSLOG installation packages for all supported platforms.

**Note:** NSLOG server is not supported on the underlying FreeBSD OS of the NetScaler appliance.

## To download NSLOG package from [www.Citrix.com](http://www.Citrix.com)

1. In a web browser, go to [www.citrix.com](http://www.citrix.com).
2. In the menu bar, click **Log In**.
3. Enter your login credentials, and then click **Log In**.
4. In the menu bar, click **Downloads**.
5. Search to find the page that provides the appropriate release number and build.
6. On that page, under **Audit Servers**, click **Download** to download the NSLOG package, having the format `AuditServer_<release number>-<build number>.zip`, to your local system (for example, `AuditServer_9.3-51.5.zip`).

## To install the NSLOG server package on a FreeBSD operating system

1. On the system to which you have downloaded the NSLOG package `AuditServer_<release number>-<build number>.zip` (for example, `AuditServer_9.3-51.5.zip`), extract the FreeBSD NSLOG server package `audserver_bsd-<release number>-<build number>.tgz` (for example, `audserver_bsd-9.3-51.5.tgz`) from the package.
2. Copy the FreeBSD NSLOG server package `audserver_bsd-<release number>-<build number>.tgz` (for example, `audserver_bsd-9.3-51.5.tgz`) to a directory on a system running FreeBSD OS.
3. At a command prompt for the directory into which the FreeBSD NSLOG server package was copied, run the following command to install the package:

```
pkg_add audserver_bsd-<release number>-<build number>.tgz
```

### Example

```
pkg_add audserver_bsd-9.3-51.5.tgz
```

The following directories are extracted:

- <root directory extracted from the FreeBSD NSLOG server package tgz file> `\netscaler\bin` (for example, `/var/auditserver/netscaler/bin`)
  - <root directory extracted from the FreeBSD NSLOG server package tgz file> `\netscaler\etc` (for example, `/var/auditserver/netscaler/etc`)
  - <root directory extracted from the FreeBSD NSLOG server package tgz file> `\netscaler\samples` (for example, `/var/auditserver/samples`)
4. At a command prompt, type the following command to verify that the package is installed:

```
pkg_info | grep NSaudserver
```

## To uninstall the NSLOG server package on a FreeBSD operating system

At a command prompt, type:

```
pkg_delete NSaudserver
```

## Installing NSLOG Server Files on the Windows Operating System

Before you can install the NSLOG server, you have to copy the NSLOG package from the NetScaler product CD or download it from [www.citrix.com](http://www.citrix.com). The NSLOG package has the following name format `AuditServer_<release number>-<build number>.zip`

(for example, `AuditServer_9.3-51.5.zip`). This package contains NSLOG installation packages for all supported platforms.

## To download NSLOG package from [www.Citrix.com](http://www.Citrix.com)

1. In a web browser, go to [www.citrix.com](http://www.citrix.com).
2. In the menu bar, click **Log In**.
3. Enter your login credentials, and then click **Log In**.
4. In the menu bar, click **Downloads**.
5. Search to find the page that provides the appropriate release number and build.
6. On that page, under **Audit Servers**, click **Download** to download the NSLOG package, having the format `AuditServer_<release number>-<build number>.zip`, to your local system (for example, `AuditServer_9.3-51.5.zip`).

## To install NSLOG server on a Windows operating system

1. On the system, where you have downloaded the NSLOG package `AuditServer_<release number>-<build number>.zip` (for example, `AuditServer_9.3-51.5.zip`), **extract** `audserver_win-<release number>-<build number>.zip` (for example, `audserver_win-9.3-51.5.zip`) from the package.
2. Copy the extracted file `audserver_<release number>-<build number>.zip` (for example, `audserver_win-9.3-51.5.zip`) to a Windows system on which you want to install the NSLOG server.
3. Unzip the `audserver_<release number>-<build number>.zip` file (for example, `audserver_win-9.3-51.5.zip`).
4. The following directories are extracted:
  - a. <root directory extracted from the Windows NSLOG server package zip file>\bin (for example, `C:\audserver_win-9.3-51.5\bin`)
  - b. <root directory extracted from the Windows NSLOG server package zip file>\etc ( for example, `C:\audserver_win-9.3-51.5\ etc` )
  - c. < root directory extracted from the Windows NSLOG server package zip file > \samples (for example, `C:\audserver_win-9.3-51.5\ samples` )
5. At a command prompt, run the following command from the <root directory extracted from the Windows NSLOG server package zip file>\bin path:  
**audserver -install -f <directorypath>\auditlog.conf**  
  
<directorypath>: Specifies the path to the configuration file ( `auditlog.conf` ). By default, `log.conf` is under <root directory extracted from Windows NSLOG server package zip file>\samples directory. But you can copy `auditlog.conf` to your desired directory.

## To uninstall the NSLOG server on a Windows operating system

At a command prompt, run the following from the <root directory extracted from Windows NSLOG server package zip file>\bin path:

```
audserver -remove
```

## NSLOG Server Command Options

The following table describes the commands that you can use to configure audit server options.

**Table 3-2. Audit Server Options**

Audit server commands	Specifies
<code>audserver -help</code>	The available Audit Server options.
<code>audserver -addns -f &lt;path to configuration file&gt;</code>	The system that gathers the log transaction data.  You are prompted to enter the IP address of the NetScaler appliance.  Enter the valid user name and password.
<code>audserver -verify -f &lt;path to configuration file&gt;</code>	Check for syntax or semantic errors in the configuration file (for example, <code>auditlog.conf</code> ).
<code>audserver -start -f &lt;path to configuration file&gt;</code>	Start audit server logging based on the settings in the configuration file ( <code>auditlog.conf</code> ).  Linux only: To start the audit server as a background process, type the ampersand sign (&) at the end of the command.
<code>audserver -stop</code> (Linux only)	Stops audit server logging when audit server is started as a background process. Alternatively, use the Ctrl+C key to stop audit server logging.
<code>audserver -install -f &lt;path to configuration file&gt;</code> (Windows only)	Installs the audit server logging client as a service on Windows.

Audit server commands	Specifies
<b>audserver -startservice</b> (Windows Only)	Start the audit server logging service, when you enter this command at a command prompt.  You can also start audit server logging from <b>Start &gt; Control Panel &gt; Services</b> .  <div style="background-color: #e6f2ff; padding: 5px;"> <p><b>Note:</b> Audit server logging starts by using the configuration settings in the configuration file, for example, <code>auditlog.conf</code> file specified in the audit server install option.</p> </div>
<b>audserver -stopservice</b> (Windows Only)	Stop audit server logging.
<b>audserver -remove</b>	Removes the audit server logging service from the registry.

Run the **audserver** command from the directory in which the audit server executable is present:

- ◆ On Windows: `\ns\bin`
- ◆ On Solaris and Linux: `\usr\local\netscaler\bin`

The audit server configuration files are present in the following directories:

- ◆ On Windows: `\ns\etc`
- ◆ On Linux: `\usr\local\netscaler\etc`

The audit server executable is started as `./auditserver` in Linux and FreeBSD.

## Adding the NetScaler Appliance IP Addresses on the NSLOG Server

In the configuration file (`auditlog.conf`), add the IP addresses of the NetScaler appliances whose events must be logged.

### To add the IP addresses of the NetScaler appliance

At a command prompt, type the following command:

```
audserver -addns -f <directorypath>\auditlog.conf
```

<directorypath>: Specifies the path to the configuration file (`auditlog.conf`).

You are prompted to enter the information for the following parameters:

NSIP: Specifies the IP address of the NetScaler appliance, for example, 10.102.29.1.

Userid: Specifies the user name, for example, nsroot.

Password: Specifies the password, for example, nsroot.

If you add multiple NetScaler IP addresses (NSIP), and later you do not want to log all of the NetScaler appliance event details, you can delete the NSIPs manually by removing the NSIP statement at the end of the `auditlog.conf` file. For a high availability (HA) setup, you must add both primary and secondary NetScaler IP addresses to `auditlog.conf` by using the `audserver` command. Before adding the IP address, make sure the user name and password exist on the system.

## Verifying the NSLOG Server Configuration File

Check the configuration file (`audit log.conf`) for syntax correctness to enable logging to start and function correctly.

To verify configuration, at a command prompt, type the following command:

```
audserver -verify -f <directorypath>\auditlog.conf
```

<directorypath>: Specifies the path to the configuration file (`audit log.conf`).

## Running the NSLOG Server

### To start audit server logging

Type the following command at a command prompt:

```
audserver -start -f <directorypath>\auditlog.conf
```

<directorypath>: Specifies the path to the configuration file (`audit log.conf`).

### To stop audit server logging that starts as a background process in FreeBSD or Linux

Type the following command:

```
audserver -stop
```

### To stop audit server logging that starts as a service in Windows

Type the following command:



```
audserver -stopservice
```

## Customizing Logging on the NSLOG Server

You can customize logging on the NSLOG server by making additional modifications to the NSLOG server configuration file (`log.conf`). Use a text editor to modify the `log.conf` configuration file on the server system.

To customize logging, use the configuration file to define filters and log properties.

- ♦ **Log filters.** Filter log information from a NetScaler appliance or a set of NetScaler appliances.
- ♦ **Log properties.** Each filter has an associated set of log properties. Log properties define how to store the filtered log information.

## Creating Filters

You can use the default filter definition located in the configuration file (`auditlog.conf`), or you can modify the filter or create a new filter. You can create more than one log filter.

**Note:** For consolidated logging, if a log transaction occurs for which there is no filter definition, the default filter is used (if it is enabled.) The only way you can configure consolidated logging of all the Citrix NetScaler appliances is by defining the default filter.

### To create a filter

At the command prompt, type the following command in the configuration file (`auditlog.conf`):

```
filter <filterName> [IP <ip>] [NETMASK <mask>] [ON | OFF]
```

<filterName>: Specify the name of the filter (maximum of 64 alphanumeric characters).

<ip>: Specify the IP addresses.

<mask>: Specify the subnet mask to be used on a subnet.

Specify ON to enable the filter to log transactions, or specify OFF to disable the filter. If no argument is specified, the filter is ON

#### Examples

```
filter F1 IP 192.168.100.151 ON
```

To apply the filter F2 to IP addresses 192.250.100.1 to 192.250.100.254:

```
filter F2 IP 192.250.100.0 NETMASK 255.255.255.0 ON
```

filterName is a required parameter if you are defining a filter with other optional parameters, such as IP address, or the combination of IP address and Netmask.

## Specifying Log Properties

Log properties associated with the filter are applied to all the log entries present in the filter. The log property definition starts with the key word BEGIN and ends with END as illustrated in the following example:

```
BEGIN <filtername>
  logFileNameFormat ...
  logDirectory ...
  logInterval ...
  logFileSizeLimit ....
END
```

Entries in the definition can include the following:

- ♦ **LogFileNameFormat** specifies the file name format of the log file. The name of the file can be of the following types:
  - **Static:** A constant string that specifies the absolute path and the file name.
  - **Dynamic:** An expression that includes the following format specifiers:
    - ♦ Date (%{format}t)
    - ♦ % creates file name with NSIP

### Example

```
LogFileNameFormat Ex%{m%d%y}t.log
```

This creates the first file name as Exmmddy.log. New files are named: Exmmddy.log.0, Exmmddy.log.1, and so on. In the following example, the new files are created when the file size reaches 100MB.

### Example

```
LogInterval size
LogFileSize 100
LogFileNameFormat Ex%{m%d%y}t
```



**Caution:** The date format %t specified in the LogFileNameFormat parameter overrides the log interval property for that filter. To prevent a new file being created every day instead of when the specified log file size is reached, do not use %t in the LogFileNameFormat parameter.

- ♦ **logDirectory** specifies the directory name format of the log file. The name of the file can be either of the following:
  - **Static:** Is a constant string that specifies the absolute path and file name.
  - **Dynamic:** Is an expression containing the following format specifiers:

- ◆ Date (%{format}t)
- ◆ % creates directory with NSIP

The directory separator depends on the operating system. In Windows, use the directory separator \.

**Example:**

```
LogDirectory dir1\dir2\dir3
```

In the other operating systems (Linux, FreeBSD, Mac, etc.), use the directory separator /.

- ◆ **LogInterval** specifies the interval at which new log files are created. Use one of the following values:
  - Hourly: A file is created every hour. Default value.
  - Daily: A file is created every day at midnight.
  - Weekly: A file is created every Sunday at midnight.
  - Monthly : A file is created on the first day of the month at midnight.
  - None: A file is created only once, when audit server logging starts.
  - Size: A file is created only when the log file size limit is reached.

**Example**

```
LogInterval Hourly
```

- ◆ **LogFileSizeLimit** specifies the maximum size (in MB) of the log file. A new file is created when the limit is reached.

Note that you can override the loginterval property by assigning size as its value.

The default LogFileSizeLimit is 10 MB.

**Example**

```
LogFileSizeLimit 35
```

## Default Settings for the Log Properties

The following is an example of the default filter with default settings for the log properties:

```
begin default
  logInterval Hourly
  logFileSizeLimit 10
  logFilenameFormat    auditlog%{%y%m%d}t.log
end default
```

Following are two examples of defining the default filters:

**Example 1**

```
Filter f1 IP 192.168.10.1
```

This creates a log file for NSI 192.168.10.1 with the default values of the log in effect.

**Example 2**

```
Filter f1 IP 192.168.10.1
begin f1
    logFilenameFormat logfiles.log
end f1
```

This creates a log file for NSIP 192.168.10.1. Since the log file name format is specified, the default values of the other log properties are in effect.

## Sample Configuration File (audit.conf)

Following is a sample configuration file:

```
#####
# This is the Auditserver configuration file
# Only the default filter is active
# Remove leading # to activate other filters
#####
MYIP <NSAuditserverIP>
MYPOR 3023
#   Filter filter_nsip  IP <Specify the NetScaler IP address to
filter on > ON
#   begin filter_nsip
#       logInterval      Hourly
#       logFileSizeLimit  10
#       logDirectory      logdir\%A\
#       logFilenameFormat nsip{%d%m%Y}t.log
#   end filter_nsip
Filter default
begin default
    logInterval      Hourly
    logFileSizeLimit  10
    logFilenameFormat  auditlog{%y%m%d}t.log
end default
```

---

## Chapter 4

# Web Server Logging

### Topics:

- [\*Configuring the NetScaler Appliance for Web Server Logging\*](#)
- [\*Installing and Configuring the Client System for Web Server Logging\*](#)
- [\*Running the NSWL Client\*](#)
- [\*Customizing Logging on the NSWL Client System\*](#)
- [\*Sample Configuration File\*](#)
- [\*Arguments for Defining a Custom Log Format\*](#)
- [\*Time Format Definition\*](#)

You can use the Web server logging feature to send logs of HTTP and HTTPS requests to a client system for storage and retrieval. This feature has two components: the Web log server, which runs on the Citrix® NetScaler® appliance, and the NetScaler Web Logging (NSWL) client, which runs on the client system. When you run the client, it connects to the NetScaler. The NetScaler buffers the HTTP and HTTPS request log entries before sending them to the NSWL client, and the client can filter the entries before storing them. You can log HTTP and HTTPS requests for all of your Web servers on one NSWL client system.

To configure Web server logging, you first enable the Web logging feature on the NetScaler and configure the size of the buffer for temporarily storing the log entries. Then, you install NSWL on the client system. You then add the NetScaler IP address (NSIP) to the NSWL configuration file. You are now ready to start the NSWL client to begin logging. You can customize Web server logging by making additional modifications to the NSWL configuration file (log.conf).

# Configuring the NetScaler Appliance for Web Server Logging

On the NetScaler appliance you need to enable the Web Server Logging feature, and you can modify the size of the buffer that stores the logged information before sending the logged information to the NetScaler Web Logging (NSWL) client.

## Enabling or Disabling Web Server Logging

Web server logging is enabled by default.

### To enable or disable Web server logging by using the NetScaler command line

At the NetScaler command prompt, type the following relevant commands to add or remove Web server logging and verify the configuration:

- ◆ **enable ns feature WL**
- ◆ **disable ns feature WL**
- ◆ **sh ns feature**

#### Example

```
> enable ns feature WL
Done
sh ns feature
```

	Feature	Acronym	Status
	-----	-----	-----
1)	<b>Web Logging</b>	<b>WL</b>	<b>ON</b>
2)	Surge Protection	SP	ON
.			
.			
.			
24)	NetScaler Push	push	OFF

```
Done
>
```

```
> disable ns feature WL
Done
sh ns feature
```

	Feature	Acronym	Status
	-----	-----	-----
1)	<b>Web Logging</b>	<b>WL</b>	<b>OFF</b>
2)	Surge Protection	SP	ON
.			
.			
.			
24)	NetScaler Push	push	OFF



Done

## To enable or disable Web server logging by using the configuration utility

1. In the navigation pane, expand **System**, and then select **Settings**.
2. In the details pane, under **Modes and Features**, click **Change advanced features**.
3. In the **Configure Advanced Features** dialog box, select the **Web Logging** check box to enable the Web logging feature, or clear the check box to disable the feature.
4. Click **OK**.
5. In the **Enable/Disable Feature(s)** dialog box, click **Yes**. A message appears in the status bar, stating that the feature has been enabled or disabled.

## Modifying the Default Buffer Size

You can change the default buffer size of 16 megabytes (MB) for Web server logging to suit your requirements. To activate your modification, you must disable and reenable Web server logging.

### To modify the buffer size by using the NetScaler command line

At the NetScaler command prompt, type the following commands to modify the buffer size and verify the configuration:

- ◆ `set weblogparam-bufferSizeMB <size>`
- ◆ `sh weblogparam`

#### Example

```
> set weblogparam -bufferSizeMB 32

> sh weblogparam
    Web Logging parameters:
    Log buffer size: 32MB

Done
```

## Parameter for modifying the buffer size

### Buffer Size

Memory (in megabytes) allocated for buffering the HTTP and HTTPS request log entries before sending them to the NSWL client.

## To modify the buffer size by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Settings**, click **Change global system settings**.
3. In the **Configure Global Settings** dialog box, under **Web Logging**, enter a value in the **Buffer\_Size (in MBytes)** text box (for example, **32**).
4. Click **OK**.

# Installing and Configuring the Client System for Web Server Logging

During installation, the NSWL client executable file (nswl) is installed along with other files. The nswl executable file includes options for performing several actions on the NSWL client, including running and stopping the NSWL client. In addition, you use the nswl executable to configure the NSWL client with the IP addresses of the NetScaler appliances from which the NSWL client will start collecting logs. Configuration settings are applied in the NSWL client configuration file (log.conf).

Then, you start the NSWL client by executing the nswl executable. The NSWL client configuration is based on the settings in the configuration file. You can further customize logging on the NSWL client system by making additional modifications to the NSLOG server configuration file (auditlog.conf).

The following table lists the operating systems on which the NSWL client is supported.

**Table 4-1. Supported Platforms for the NSWL Client**

Operating system	Version
Windows	<ul style="list-style-type: none"> <li>◆ Windows XP Professional</li> <li>◆ Windows Server 2003</li> <li>◆ Windows 2000/NT</li> <li>◆ Windows Server 2008</li> <li>◆ Windows Server 2008 R2</li> </ul>
Mac OS	Mac OS 8.6 or later
Linux	<ul style="list-style-type: none"> <li>◆ RedHat Linux 4 or later</li> <li>◆ SUSE Linux Enterprise 9.3 or later</li> </ul>
Solaris	Solaris Sun OS 5.6 or later



Operating system	Version
FreeBSD	FreeBSD 6.3 or later

The following table describes the minimum hardware specifications for the platform running the NSWL client.

**Table 4-2. Minimum Hardware Specification for Platforms Running the NSWL Client**

Operating system	Hardware requirements
For Windows / Linux / FreeBSD	<ul style="list-style-type: none"> <li>• Processor- Intel x86 -501 megahertz (MHz)</li> <li>• RAM - 512 megabytes (MB)</li> <li>• Controller - SCSI</li> </ul>
For Solaris 2.6	<ul style="list-style-type: none"> <li>• Processor - UltraSPARC-III 400 MHz</li> <li>• RAM - 512 MB</li> <li>• Controller - SCSI</li> </ul>

If the NSWL client system cannot process the log transaction because of a CPU limitation, the Web log buffer overruns and the logging process reinitiates.



**Caution:** Reinitiation of logging can result in loss of log transactions.

To temporarily solve a NSWL client system bottleneck caused by a CPU limitation, you can tune the Web server logging buffer size on the NetScaler appliance. To solve the problem, you need a client system that can handle the site's throughput.

## Installing NSWL Client on a Solaris Operating System

Copy the installation files from the NetScaler product CD or download them from [ftp.netscaler.com](http://ftp.netscaler.com). Log on to the Solaris system as an administrator. Use the following procedure to install the NSWL executable and the other files on the system.

### To install the NSWL client package on a Solaris operating system

1. At a command prompt, copy the NSweblog.tar file into a temporary directory using the command:

```
cp <path_to_cd>/Utilities/weblog/Solaris/NSweblog.tar /tmp
```

2. Change to the temporary directory:

```
cd /tmp
```

3. Extract the files from the \*.tar file with the following command:

```
tar xvf NSweblog.tar
```

A directory NSweblog is created in the temporary directory, and the files are extracted to the NSweblog directory.

4. Install the package with the following command:

```
pkgadd -d
```

The list of available packages appears. In the following example, one NSweblog package is shown:

```
1 NSweblog NetScaler Weblogging
(SunOS, sparc) 7.0
```

5. You are prompted to select the packages. Select the package number of the NSweblog to be installed.

After you select the package number and press Enter, the files are extracted and installed in the following directories:

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

6. At a command prompt, type the following command to check whether the package is installed:

```
pkginfo | grep NSweblog
```

## To uninstall the NSWL client package on a Solaris operating system

At a command prompt, type:

```
pkgrm NSweblog
```

## Installing NSWL Client on a Linux Operating System

Copy the installation files from the NetScaler product CD or download them from [ftp.netscaler.com](http://ftp.netscaler.com). Log on to the Linux system as an administrator. Use the following procedure to install the NSWL executable and the other files on the system.

### To install the NSWL client package on a Linux operating system

1. At a command prompt, copy the NSweblog.rpm file into a temporary directory:

```
cp <path_to_cd>/Utilities/weblog/Linux/NSweblog.rpm /tmp
```

2. To install the NSWL executable, use the following command:

```
rpm -i NSweblog.rpm
```

This command extracts the files and installs them in the following directories.

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

### **To uninstall the NSWL client package on a Linux operating system**

At a command prompt, type:

```
rpm -e NSweblog
```

### **To get more information about the NSweblog RPM file**

At a command prompt, type:

```
rpm -qpi *.rpm
```

### **To view the installed Web server logging files**

At a command prompt, type:

```
rpm -qpl *.rpm
```

## **Installing NSWL Client on a FreeBSD Operating System**

Copy the installation files from the NetScaler product CD or download them from [ftp.netscaler.com](http://ftp.netscaler.com). Log on to the FreeBSD system as an administrator. Use the following procedure to install the NSWL executable and the other files on the system.

### **To install the NSWL client package on a FreeBSD operating system**

1. At a command prompt, copy the NSweblog.tgz file into a temporary directory:

```
cp <path_to_cd>/Utilities/weblog/Freebsd/NSweblog.tgz /tmp
```

2. Change to the temporary directory:

```
cd /tmp
```

3. Install the package using the following command:

```
pkg_add NSweblog.tgz
```

This command extracts the files and installs them in the following directories.

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

4. To verify that the package is installed, use the following command:

```
pkg_info | grep NSweblog
```

### **To uninstall the NSWL client package on a FreeBSD operating system**

At a command prompt, type:

```
pkg_delete NSweblog
```

## **Installing NSWL Client on a Mac OS Operating System**

Copy the installation files from the NetScaler product CD or download them from [ftp.netscaler.com](http://ftp.netscaler.com). Log on to the Mac OS operating system as an administrator. Use the following procedure to install the NSWL executable and the other files on the system.

### **To install the NSWL client package on a Mac OS operating system**

1. At a command prompt, copy the NSweblog.tgz file into a temporary directory with the following command:

```
cp <path_to_cd>/Utilities/weblog/macos/NSweblog.tgz /tmp
```

2. Change to the temporary directory:

```
cd /tmp
```

3. To install the package, use the pkg\_add command:

```
pkg_add NSweblog.tgz
```

This command extracts the files and installs them in the following directories:

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

4. To verify that the package is installed, use the following command:

```
pkg_info | grep NSweblog
```

## To uninstall the NSWL client package on a Mac OS operating system

At a command prompt, type:

```
pkg_delete NSweblog
```

## Installing NSWL Client on a Windows Operating System

Before installing the NSWL client, you have to copy the NSWL client package from the NetScaler product CD or download it from [www.citrix.com](http://www.citrix.com). The NSWL client package has the following name format:

Weblog\_<release number>-<build number>.zip (for example, Weblog\_9.3-51.5.zip). Within the package are separate installation packages for each supported platforms.

### To download NSWL client package from [www.Citrix.com](http://www.Citrix.com)

1. From any system, open [www.citrix.com](http://www.citrix.com) in the Web browser.
2. In the menu bar, click **Log In**.
3. Enter your login credentials and then click **Log In**.
4. In the menu bar, click **Downloads**.
5. Search to the page of the desired release number and build.
6. On the desired page, under **Weblog Clients**, click **Download** to download a file, having the format Weblog\_<release number>-<build number>.zip, to your local system (for example, Weblog\_9.3-51.5.zip).

### To install the NSWL client on a Windows system

1. On the system, where you have downloaded the NSWL client package Weblog\_<release number>-<build number>.zip (for example, Weblog\_9.3-51.5.zip), extract nswl\_win-<release number>-<build number>.zip (for example, nswl\_win-9.3-51.5.zip) from the package.
2. Copy the extracted file nswl\_win-<release number>-<build number>.zip (for example, nswl\_win-9.3-51.5.zip) to a Windows system on which you want to install the NSWL client.
3. On the Windows system, unzip the nswl\_<release number>-<build number>.zip file (for example, nswl\_win-9.3-51.5.zip). The following directories are extracted:
  - a. <root directory extracted from the Windows NSWL client package zip file>\bin (for example, C:\nswl\_win-9.3-51.5\bin)

- b. <root directory extracted from the Windows NSWL client package zip file>\etc (for example, C:\nswl\_win-9.3-51.5\ etc )
  - c. < root directory extracted from the Windows NSWL client package zip file >\samples (for example, C:\nswl\_win-9.3-51.5\samples )
4. At a command prompt, run the following command from the <root directory extracted from the Windows NSWL client package zip file>\bin path:

```
nswl -install -f <directorypath> \log.conf
```

<directorypath>: Specifies the path to the configuration file ( log.conf ). By default, log.conf is in the < root directory extracted from the Windows NSWL client package zip file >\samples directory. But you can copy log.conf to your desired directory.

### To uninstall the NSWL client on a Windows system

At a command prompt, run the following from the <root directory extracted from the Windows NSWL client package zip file>\bin path:

```
nswl -remove
```

## Installing NSWL Client on an AIX Operating System

Copy the installation files from the NetScaler product CD or download them from ftp.netscaler.com. Log on to the AIX system as an administrator. Use the following procedure to install the NSWL executable and the other files on the system.

### To install the NSWL client package on an AIX operating system

1. Copy the NSweblog.rpm file into a temporary directory:

```
cp <path_to_cd>/Utilities/weblog/AIX/NSweblog.rpm /tmp
```

2. To install the NSWL executable, use the following command:

```
rpm -i NSweblog.rpm
```

This command extracts the files and installs them in the following directories.

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

### To uninstall the NSWL client package on an AIX operating system

At a command prompt, type:

```
rpm -e NSweblog
```

### To get more information about the NSweblog RPM file

At a command prompt, type:

```
rpm -qpi *.rpm
```

### To view the installed Web server logging files

At a command prompt, type:

```
rpm -qpl *.rpm
```

## NSWL Client Command Options

The following table describes the commands that you can use to configure the NSWL client.

**Table 4-3. NSWL Command Options**

NSWL command	Specifies
<code>nswl -help</code>	The available NSWL help options.
<code>nswl -addns -f &lt;path to configuration file&gt;</code>	The system that gathers the log transaction data. You are prompted to enter the IP address of the NetScaler appliance. Enter a valid user name and password.
<code>nswl -verify -f &lt;path to configuration file&gt;</code>	Check for syntax or semantic errors in the configuration file (for example, <code>log.conf</code> ).
<code>nswl -start -f &lt;path to configuration file&gt;</code>	Start the NSWL client based on the settings in the configuration file (for example, <code>log.conf</code> ). For Solaris and Linux: To start Web server logging as a background process, type the ampersand sign (&) at the end of the command.
<code>nswl -stop</code> (Solaris and Linux only)	Stop the NSWL client if it was started as a background process; otherwise, use CTRL+C to stop Web server logging.
<code>nswl -install -f &lt;path to configuration file&gt;</code> (Windows only)	Install the NSWL client as a service in Windows.
<code>nswl -startservice</code> (Windows only)	Start the NSWL client by using the settings in the configuration file (for example, <code>log.conf</code> ) specified in the <code>nswl</code>

NSWL command	Specifies
	install option. You can also start NSWL client from <b>Start &gt; Control Panel &gt; Services</b> .
nswl -stopservice (Windows only)	Stops the NSWL client.
nswl -remove	Remove the NSWL client service from the registry.

Run the following commands from the directory in which the NSWL executable is located:

- ♦ Windows: \ns\bin
- ♦ Solaris and Linux: \usr\local\netscaler\bin

The Web server logging configuration files are located in the following directory path:

- ♦ Windows: \ns\etc
- ♦ Solaris and Linux: \usr\local\netscaler\etc

The NSWL executable is started as .nswl in Linux and Solaris.

## Adding the IP Addresses of the NetScaler Appliance

In the NSWL client configuration file (log.conf), add the NetScaler IP address (NSIP) from which the NSWL client will start collecting logs.

### To add the NSIP address of the NetScaler appliance

1. At the client system command prompt, type:

```
nswl -addns -f < directorypath > \log.conf
```

< directorypath >: Specifies the path to the configuration file (log.conf).

2. At the next prompt, enter the following information:

- NSIP: Specify the IP address of the NetScaler appliance.
- User name: Specify the user name of the NetScaler appliance.
- Password: Specify the password.

**Note:** If you add multiple NetScaler IP addresses (NSIP), and later you do not want to log all of NetScaler system log details, you can delete the NSIPs manually by removing the NSIP statement at the end of the log.conf file. During a failover setup, you must add both primary and secondary NetScaler IP addresses to the log.conf by using the command. Before adding the IP address, make sure the user name and password exist on the NetScaler appliances.



## Verifying the NSWL Configuration File

To make sure that logging works correctly, check the NSWL configuration file (log.conf) on the client system for syntax errors.

### To verify the configuration in the NSWL configuration file

At the client system command prompt, type:

```
nswl -verify -f <directorypath>\log.conf
```

< directorypath >: Specifies the path to the configuration file (log.conf).

## Running the NSWL Client

### To start Web server logging

At the client system command prompt, type:

```
nswl -start -f <directorypath>\log.conf
```

<directorypath>: Specifies the path to the configuration file ( log.conf).

### To stop Web server logging started as a background process on the Solaris or Linux operating systems

At the command prompt, type:

```
nswl -stop
```

### To stop Web server logging started as a service on the Windows operating system

At the command prompt, type:

```
nswl -stopservice
```

## Customizing Logging on the NSWL Client System

You can customize logging on the NSWL client system by making additional modifications to the NSWL client configuration file (log.conf). Use a text editor to modify the log.conf configuration file on the client system.

To customize logging, use the configuration file to define filters and log properties.

- ♦ **Log filters.** Filter log information based on the host IP address, domain name, and host name of the Web servers.
- ♦ **Log properties.** Each filter has an associated set of log properties. Log properties define how to store the filtered log information.

## Creating Filters

You can use the default filter definition located in the configuration file ( `log.conf`), or you can modify the filter or create a new filter. You can create more than one log filter.

**Note:** Consolidated logging, which logs transactions for which no filter is defined, uses the default filter if it is enabled. Consolidated logging of all servers can be done by defining only the default filter.

If the server hosts multiple Web sites and each Web site has its own domain name, and each domain is associated with a virtual server, you can configure Web server logging to create a separate log directory for each Web site. The following table displays the parameters for creating a filter.

**Table 4-4. Parameters for Creating a Filter**

Parameter	Specifies
filterName	Name of the filter (maximum 64 alphanumeric characters).
HOST name	Host name of the server for which the transactions are being logged.
IP ip	IP address of the server for which transactions are to be logged (for example, if the server has multiple domains that have one IP address).
IP ip 2...ip n:	Multiple IP addresses (for example, if the server domain has multiple IP addresses).
ip6 ip	IPv6 address of the server for which transactions are to be logged.
IP ip NETMASK mask	IP addresses and netmask combination to be used on a subnet.
ON   OFF	Enable or disable the filter to log transactions. If no argument is selected, the filter is enabled (ON).

## To create a filter

To create a filter, enter the following command in the log.conf file:

- ♦ `filter <filterName> <HOST name> | [IP <ip>] | [IP <ip 2...ip n>] | <IP ip NETMASK mask> [ON | OFF]`
- ♦ `filter <filterName> <HOST name> | [IP6 ip/<prefix length>] [ON | OFF]`

## To create a filter for a virtual server

To create a filter for a virtual server, enter the following command in the log.conf file:

`filter <filterName> <VirtualServer IP address>`

### Example

In the following example, you specify an IP address of 192.168.100.0 and netmask of 255.255.255.0. The filter applies to IP addresses 192.168.100.1 through 192.168.100.254.

```
Filter F1 HOST www.netscaler.com ON
Filter F2 HOST www.netscaler.com IP 192.168.100.151
ON
Filter F3 HOST www.netscaler.com IP 192.168.100.151
192.165.100.152 ON
Filter F4 IP 192.168.100.151
Filter F5 IP 192.168.100.151 HOST www.netscaler.com
OFF
Filter F6 HOST www.netscaler.com HOST www.xyz.com
HOST www.abcxyz.com IP 192.168.100.200 ON
Filter F7 IP 192.250.100.0 NETMASK 255.255.255.0
Filter F8 HOST www.xyz.com IP 192.250.100.0 NETMASK
255.255.255.0 OFF
For creating filters for servers having IPv6
addresses.
Filter F9 2002::8/112 ON
Filter F10 HOST www.abcd.com IP6 2002::8 ON
```

## Specifying Log Properties

Log properties are applied to all log entries associated with the filter. The log property definition begins with the keyword BEGIN and ends with END as illustrated in the following example:

```
BEGIN <filtername>
logFormat ...
logFilenameFormat ...
logInterval ...
logFileSize ....
logExclude ....
logTime ...
END
```

Entries in the definition can include the following:

- ◆ **LogFormat** specifies the Web server logging feature that supports NCSA, W3C Extended, and custom log file formats.

By default, the logformat property is w3c. To override, enter custom or NCSA in the configuration file, for example:

```
LogFormat NCSA
```

**Note:** For the NCSA and custom log formats, local time is used to time stamp transactions and for file rotation.

- ◆ **LogInterval** specifies the intervals at which new log files are created. Use one of the following values:
  - Hourly: A file is created every hour.
  - Daily: A file is created every day at midnight. Default value.
  - Weekly: A file is created every Sunday at midnight.
  - Monthly: A file is created on the first day of the month at midnight.
  - None: A file is created only once, when Web server logging starts.

**Example**

```
LogInterval Daily
```

- ◆ **LogFileSizeLimit** specifies the maximum size of the log file in MB. It can be used with any log interval (weekly, monthly, and so on.) A file is created when the maximum file size limit is reached or when the defined log interval time elapses.

To override this behavior, specify the size as the loginterval property so that a file is created only when the log file size limit is reached.

The default LogFileSizeLimit is 10 MB.

**Example**

```
LogFileSizeLimit 35
```

- ◆ **LogFilenameFormat** specifies the file name format of the log file. The name of the file can be of the following types:
  - Static: Specifies a constant string that contains the absolute path and file name.
  - Dynamic: Specifies an expression containing the following format:
    - ◆ Server IP address (%A)
    - ◆ Date (%{format}t)
    - ◆ URL suffix (%x)
    - ◆ Host name (%v)

**Example**

```
LogFileFormat Ex{%m%d%y}t.log
```

This command creates the first file name as Exmddyy.log, then every hour creates a file with file name: Exmddyy.log.0, Exmddyy.log.1,..., Exmddyy.log.n.

**Example**

```
LogInterval size
LogFileSize 100
LogFileFormat Ex{%m%d%y}t
```



**Caution:** The date format %t specified in the LogFilenameFormat command overrides the log interval property for that filter. To prevent a new file being created every day instead of when the specified log file size is reached, do not use %t in the LogFilenameFormat.

- ◆ **LogExclude** prevents logging of transactions with the specified file extensions.

**Example**

```
LogExclude .html
```

This command creates a log file that excludes log transactions for \*.html files.

- ◆ **LogTime** specifies log time as either GMT or LOCAL.

The defaults are:

- NCSA log file format: LOCAL
- W3C log file format: GMT.

## Understanding the NCSA and W3C Log Formats

The NetScaler supports the following standard log file formats:

- ◆ NCSA Common Log Format
- ◆ W3C Extended Log Format

### NCSA Common Log Format

If the log file format is NCSA, the log file displays log information in the following format:

```
Client_IP_address -User_Name [Date:Time -TimeZone] "Method
Object HTTP_version" HTTP_StatusCode BytesSent
```

To use the NCSA Common log format, enter NCSA in the LogFormat argument in the log.conf file.

The following table describes the NCSA Common log format.

**Table 4-5. NCSA Common Log Format**

Argument	Specifies
Client_IP_address	The IP address of the client computer.
User Name	The user name.
Date	The date of the transaction.
Time	The time when the transaction was completed.
Time Zone	The time zone (Greenwich Mean Time or local time).
Method	The request method (for example; GET, POST).
Object	The URL.
HTTP_version	The version of HTTP used by the client.
HTTP_StatusCode	The status code in the response.
Bytes Sent	The number of bytes sent from the server.

## W3C Extended Log Format

An extended log file contains a sequence of lines containing ASCII characters terminated by either a Line Feed (LF) or the sequence Carriage Return Line Feed (CRLF.) Log file generators must follow the line termination convention for the platform on which they are run.

Log analyzers must accept either LF or CRLF form. Each line may contain either a directive or an entry. If you want to use the W3C Extended log format, enter W3C as the Log-Format argument in the log.conf file.

By default, the standard W3C log format is defined internally as the custom log format, shown as follows:

```
%{%Y-%m-%d%H:%M:%S}t %a %u %S %A %p %m %U %q %s %j %J %T %H %+
{user-agent}i %+{cookie} i%+{referer}i
```

For a description of the meaning of this each custom format, see [Arguments for Defining a Custom Log Format](#) on page 118. You can also change the order or remove some fields in this W3C log format. For example:

```
logFormat W3C {%Y-%m-%d%H:%M:%S}t %m %U
```

W3C log entries are created with the following format:

```
#Version: 1.0
#Fields: date time cs-method cs-uri
#Date: 12-Jun-2001 12:34
```

```
2001-06-12 12:34:23 GET /sports/football.html
2001-06-12 12:34:30 GET /sports/football.html
```

## Entries

Entries consist of a sequence of fields relating to a single HTTP transaction. Fields are separated by white space; Citrix recommends the use of tab characters. If a field in a particular entry is not used, a dash (-) marks the omitted field.

## Directives

Directives record information about the logging process. Lines beginning with the pound sign (#) contain directives.

The following table describes the directives.

**Table 4-6. Directive Descriptions**

Directive	Description
Version: <integer>.<integer>	Displays the version of the extended log file format used. This document defines version 1.0.
Fields: [<specifier>...]	Identifies the fields recorded in the log.
Software: <string>	Identifies the software that generated the log.
Start-Date: <date> <time>	Displays the date and time at which the log was started.
End-Date: <date> <time>	Displays the date and time at which logging finished.
Date: <date> <time>	Displays the date and time when the entry was added.
Remark: <text>	Displays comments. Analysis tools ignore data recorded in this field.

**Note:** The Version and Fields directives are required. They precede all other entries in the log file.

## Example

The following sample log file shows the log entries in W3C Extended log format:

```
#Version: 1.0
#Fields: time cs-method cs-uri
#Date: 12-Jan-1996 00:00:00
00:34:23 GET /sports/football.html
12:21:16 GET /sports/football.html
```

```
12:45:52 GET /sports/football.html
12:57:34 GET /sports/football.html
```

## Fields

The Fields directive lists a sequence of field identifiers that specify the information recorded in each entry. Field identifiers may have one of the following forms:

- ♦ **identifier:** Relates to the transaction as a whole.
- ♦ **prefix-identifier:** Relates to information transfer between parties defined by the value *prefix*.
- ♦ **prefix (header):** Specifies the value of the HTTP header field header for transfer between parties defined by the value *prefix*. Fields specified in this manner always have the type <string>.

The following table describes defined prefixes.

**Table 4-7. Prefix Descriptions**

Prefix	Specifies
c	Client
s	Server
r	Remote
cs	Client to server
sc	Server to client
sr	Server to remote server (prefix used by proxies)
rs	Remote server to server (prefix used by proxies)
x	Application-specific identifier

### Examples

The following examples are defined identifiers that use prefixes:

**cs-method:** The method in the request sent by the client to the server.

**sc(Referer):** The Referer field in the reply.

**c-ip:** The IP address of the client.

## Identifiers

The following table describes the W3C Extended log format identifiers that do not require a prefix.



**Table 4-8. W3C Extended Log Format Identifiers (No Prefix Required)**

Identifier	Description
date	The date on which the transaction was done.
time	The time when the transaction is done.
time-taken	The time taken (in seconds) for the transaction to complete.
bytes	The number of bytes transferred.
cached	Records whether a cache hit has occurred. A zero indicates a cache miss.

The following table describes the W3C Extended log format identifiers that require a prefix.

**Table 4-9. W3C Extended Log Format Identifiers (Requires a Prefix)**

Identifier	Description
IP	The IP address and the port number.
dns	The DNS name.
status	The status code.
comment	The comment returned with status code.
method	The method.
url	The URL.
url-stem	The stem portion of the URL.
url-query	The query portion of the URL.

The W3C Extended Log file format allows you to choose log fields. These fields are shown in the following table.

**Table 4-10. W3C Extended Log File Format (Allows Log Fields)**

Field	Description
Date	The date on which the transaction is done.
Time	The time when the transaction is done.
Client IP	The IP address of the client.

Field	Description
User Name	The user name.
Service Name	The service name, which is always HTTP.
Server IP	The server IP address.
Server Port	The server port number
Method	The request method (for example; GET, POST).
Url Stem	The URL stem.
Url Query	The query portion of the URL.
Http Status	The status code in the response.
Bytes Sent	The number of bytes sent to the server (request size, including HTTP headers).
Bytes Received	The number of bytes received from the server (response size, including HTTP headers).
Time Taken	The time taken for transaction to complete, in seconds.
Protocol Version	The version number of HTTP being used by the client.
User Agent	The User-Agent field in the HTTP protocol.
Cookie	The Cookie field of the HTTP protocol.
Referer	The Referer field of the HTTP protocol.

## Creating a Custom Log Format

You can customize the display format of the log file data manually or by using the NSWL library. By using the custom log format, you can derive most of the log formats that Apache currently supports.

### Creating a Custom Log Format by Using the NSWL Library

Use one of the following NSWL libraries depending on whether the NSWL executable has been installed on a Windows or Solaris host computer:

- ♦ **Windows:** The `nswl.lib` library located in `\ns\bin` directory on the system manager host computer.

- ◆ **Solaris:** The libnswl.a library located in /usr/local/netscaler/bin.

### To create the custom log format by using the NSWL Library

1. Add the following two C functions defined by the system in a C source file:
  - ns\_userDefFieldName() : This function returns the string that must be added as a custom field name in the log record.
  - ns\_userDefFieldVal() : This function implements the custom field value, then returns it as a string that must be added at the end of the log record.
2. Compile the file into an object file.
3. Link the object file with the NSWL library (and optionally, with third party libraries) to form a new NSWL executable.
4. Add a %d string at the end of the logFormat string in the configuration file (log.conf).

#### Example

```
#####
# A new file is created every midnight or on
# reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/
NS<hostname>/Nsmdddy.log and create digital
#signature field for each record.
BEGIN CACHE_F
    logFormat      custom "%a - %{user-agent}i" [%d/
%B/%Y %T -%g] "%x" %s %b%{referrer}i "%{user-
agent}i" "%{cookie}i" %d "
    logInterval    Daily
    logFileSizeLimit      20
    logFilenameFormat    /datadisk5/netscaler/
log/%v/NS%{m%d%y}t.log
END CACHE_F
```

## Creating a Custom Log Format Manually

To customize the format in which log file data should appear, specify a character string as the argument of the LogFormat log property definition. For more information, see [Arguments for Defining a Custom Log Format](#) on page 118. The following is an example where character strings are used to create a log format:

```
LogFormat Custom "%a - %{user-agent}i" [%d/%m/%Y]t %U %s %b
%T"
```

- ◆ The string can contain the “c” type control characters \n and \t to represent new lines and tabs.
- ◆ Use the <Esc> key with literal quotes and backslashes.

The characteristics of the request are logged by placing % directives in the format string, which are replaced in the log file by the values.


If the %v (Host name) or %x (URL suffix) format specifier is present in a log file name format string, the following characters in the file name are replaced by an underscore symbol in the log configuration file name:

```
" * . / : < > ? \ |
```

Characters whose ASCII values lie in the range of 0-31 are replaced by the following:

```
%<ASCII value of character in hexadecimal>.
```

For example, the character with ASCII value 22 is replaced by %16.

 **Caution:** If the %v format specifier is present in a log file name format string, a separate file is opened for each virtual host. To ensure continuous logging, the maximum number of files that a process can have open should be sufficiently large. See your operating system documentation for a procedure to change the number of files that can be opened.

## Creating Apache Log Formats

You can derive from the custom logs most of the log formats that Apache currently supports. The custom log formats that match Apache log formats are:

NCSA/combined: LogFormat custom %h %l %u [%t] "%r" %s %B "%{referer}i" "%{user-agent}i"

NCSA/Common: LogFormat custom %h %l %u [%t] "%r" %s %B

Referer Log: LogFormat custom "%{referer}i" -> %U

Useragent: LogFormat custom %{user-agent}i

Similarly, you can derive the other server log formats from the custom formats.

## Sample Configuration File

Following is a sample configuration file:

```
#####
# This is the NSWL configuration file
# Only the default filter is active
# Remove leading # to activate other filters
#####
#####
# Default filter (default on)
# W3C Format logging, new file is created every hour or on
reaching 10MB file size,
# and the file name is Exyymmdd.log
#####
Filter default
begin default
    logFormat                W3C
    logInterval               Hourly
    logFileSizeLimit         10
```

```

        logFilenameFormat      Ex{%y%m%d}t.log
end default
#####
# netscaler caches example
# CACHE_F filter covers all the transaction with HOST name
www.netscaler.com and the listed server ip's
#####
#Filter CACHE_F HOST www.netscaler.com IP 192.168.100.89
192.168.100.95 192.168.100.52 192.168.100.53 ON
#####
# netscaler origin server example
# Not interested in Origin server to Cache traffic transaction
logging
#####
#Filter ORIGIN_SERVERS IP 192.168.100.64 192.168.100.65
192.168.100.66 192.168.100.67 192.168.100.225 192.168.100.226
192.168.
100.227 192.168.100.228 OFF
#####
# netscaler image server example
# all the image server logging.
#####
#Filter IMAGE_SERVER HOST www.netscaler.images.com IP
192.168.100.71 192.168.100.72 192.168.100.169 192.168.100.170
192.168.10
0.171 ON
#####
# NCSA Format logging, new file is created every day midnight or
on reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/
Nsmddyy.log.
# Exclude objects that ends with .gif .jpg .jar.
#####
#begin ORIGIN_SERVERS
#       logFormat           NCSA
#       logInterval         Daily
#       logFileSizeLimit    40
#       logFilenameFormat   /datadisk5/ORGIN/log/%v/NS{%m%d
%y}t.log
#       logExclude          .gif .jpg .jar
#end ORIGIN_SERVERS

#####
# NCSA Format logging, new file is created every day midnight or
on reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/
Nsmddyy.log with log record timestamp as GMT.
#####
#begin CACHE_F
#       logFormat           NCSA
#       logInterval         Daily
#       logFileSizeLimit    20
#       logFilenameFormat   /datadisk5/netscaler/log/%v/NS{%m%d
%y}t.log
#       logtime             GMT
#end CACHE_F

```

```
#####
# W3C Format logging, new file on reaching 20MB and the log file
path name is
# atadisk6/netScaler/log/server's ip/Exmmydd.log with log record
timestamp as LOCAL.
#####
#begin IMAGE_SERVER
#     logFormat           W3C
#     logInterval         Size
#     logFileSizeLimit    20
#     logFilenameFormat  /datadisk6/netScaler/log/%AEx{%m%d%y}t
#     logtime              LOCAL
#end IMAGE_SERVER

#####
# Virtual Host by Name firm, can filter out the logging based on
the host name by,
#####

#Filter VHOST_F IP 10.101.2.151 NETMASK 255.255.255.0
#begin VHOST_F
#     logFormat           W3C
#     logInterval         Daily
#     logFileSizeLimit    10
logFilenameFormat /ns/prod/vhost/%v/Ex{%m%d%y}t
#end VHOST_F

##### END FILTER CONFIGURATION #####
```

## Arguments for Defining a Custom Log Format

The following table describes the data that you can use as the Log Format argument string:

**Table 4-11. Custom Log Format**

Argument	Specifies
%a	The remote IPv4 address.
%A	The local IPv4 address.
%a6	The remote IPv6 address.
%A6	The local IPv6 address.
%B	The bytes sent, excluding the HTTP headers (response size).

Argument	Specifies
%b	The bytes received, excluding the HTTP headers (request size).
%d	A user-defined field.
%g	The Greenwich Mean Time offset (for example, -0800 for Pacific Standard Time).
%h	The remote host.
%H	The request protocol.
%{Foobar}i	The contents of the Foobar: header line(s) in the request sent to the server. The system supports the User-Agent, Referer and cookie headers. The + after the % in this format informs the logging client to use the + as a word separator.
%j	The bytes received, including headers (request size)
%J	The bytes sent, including headers (response size)
%l	The remote log name (from identd, if supplied).
%m	The request method.
%M	The time taken to serve the request (in microseconds)
%{Foobar}o	The contents of Foobar: header line(s) in the reply. USER-AGENT, Referer, and cookie headers are supported.
%p	The canonical port of the server serving the request.
%q	The query string (prefixed with a question mark (?) if a query string exists).

Argument	Specifies
%r	The first line of the request.
%s	For requests that were redirected internally, this is the status of the original request.
%t	The time, in common log format (standard English time format).
%{format}t	The time, in the form given by format, must be in the strftime(3) format. For format descriptions, see <a href="#">Time Format Definition</a> on page 121.
%T	The time taken to serve the request, in seconds.
%u	The remote user (from auth; may be bogus if return status (%s) is 401).
%U	The URL path requested.
%v	The canonical name of the server serving the request.
%V	This is the virtual server IPv4 address in the system, if load balancing, content switching, and/or cache redirection is used.
%V6	This is the virtual server IPv6 address in the system, if load balancing, content switching, and/or cache redirection is used.

For example, if you define the log format as `%+{user-agent}i`, and if the user agent value is Citrix NetScaler system Web Client, then the information is logged as Citrix NetScaler system +Web+Client. An alternative is to use double quotation marks. For example, `"%{user-agent}i"` logs it as "Citrix NetScaler system Web Client." Do not use the <Esc> key on strings from `%.. .r`, `%.. .i` and `%.. .o`. This complies with the requirements of the Common Log Format. Note that clients can insert control characters into the log. Therefore, you should take care when working with raw log files.



## Time Format Definition

The following table lists the characters that you can enter as the format part of the `{format}t` string described in the Custom Log Format table of [Arguments for Defining a Custom Log Format](#) on page 118. Values within brackets ([ ]) show the range of values that appear. For example, [1,31] in the `%d` description in the following table shows `%d` ranges from 1 to 31.

**Table 4-12. Time Format Definition**

Argument	Specifies
<code>%%</code>	The same as <code>%</code> .
<code>%a</code>	The abbreviated name of the week day for the locale.
<code>%A</code>	The full name of the week day for the locale.
<code>%b</code>	The abbreviated name of the month for the locale.
<code>%B</code>	The full name of the month for the locale.
<code>%C</code>	The century number (the year divided by 100 and truncated to an integer as a decimal number [1,99]); single digits are preceded by a 0.
<code>%d</code>	The day of month [1,31]; single digits are preceded by 0.
<code>%e</code>	The day of month [1,31]; single digits are preceded by a blank.
<code>%h</code>	The abbreviated name of the month for the locale.
<code>%H</code>	The hour (24-hour clock) [0,23]; single digits are preceded by a 0.
<code>%I</code>	The hour (12-hour clock) [1,12]; single digits are preceded by a 0.
<code>%j</code>	The number of the day in the year [1,366]; single digits are preceded by 0.
<code>%k</code>	The hour (24-hour clock) [0,23]; single digits are preceded by a blank.

Argument	Specifies
%l	The hour (12-hour clock) [1,12]; single digits are preceded by a blank.
%m	The number of the month in the year [1,12]; single digits are preceded by a 0.
%M	The minute [00,59]; leading 0 is permitted but not required.
%n	Inserts a new line.
%p	The equivalent of either a.m. or p.m. for the locale.
%r	The appropriate time representation in 12-hour clock format with %p.
%S	The seconds [00,61]; the range of values is [00,61] rather than [00,59] to allow for the occasional leap second and for the double leap second.
%t	Inserts a tab.
%u	The day of the week as a decimal number [1,7]. 1 represents Sunday, 2 represents Tuesday and so on.
%U	The number of the week in the year as a decimal number [00,53], with Sunday as the first day of week 1.
%w	The day of the week as a decimal number [0,6]. 0 represents Sunday.
%W	Specifies the number of the week in the year as a decimal number [00,53]. Monday is the first day of week 1.
%y	The number of the year within the century [00,99]. For example, 5 would be the fifth year of that century.
%Y	The year, including the century (for example, 1993).

**Note:** If you specify a conversion that does not correspond to any of the ones described in the preceding table, or to any of the modified conversion specifications listed in the next paragraph, the behavior is undefined and returns 0.

The difference between %U and %W (and also between modified conversions %OU and %OW) is the day considered to be the first day of the week. Week number 1 is the first week in January (starting with a Sunday for %U, or a Monday for %W). Week number 0 contains the days before the first Sunday or Monday in January for %U and %W.



---

## Chapter 5

# Advanced Configurations

### Topics:

- [\*Configuring Clock Synchronization\*](#)
- [\*Viewing the System Date and Time\*](#)
- [\*Configuring TCP Window Scaling\*](#)
- [\*Configuring Selective Acknowledgment\*](#)
- [\*Clearing the Configuration\*](#)
- [\*Viewing the HTTP Band Statistics\*](#)
- [\*Configuring HTTP Profiles\*](#)
- [\*Configuring TCP Profiles\*](#)
- [\*Specifying a TCP Buffer Size\*](#)
- [\*Optimizing the TCP Maximum Segment Size for a Virtual Server Configuration\*](#)

You can configure network time protocol to synchronize a Citrix® NetScaler® appliance's local clock with the other servers on the network. If you enable path maximum transmission unit (PMTU) discovery, the NetScaler can use it to determine the maximum transmission unit of any Internet channel. For more efficient data transfer, you can configure TCP window scaling and selective acknowledgment. You can clear any basic or extended configuration on your NetScaler. You can view statistics associated with HTTP request and response sizes. For applying a specific HTTP and TCP settings to vservers and services, you can configure HTTP and TCP profiles.

## Configuring Clock Synchronization

You can configure your NetScaler appliance to synchronize its local clock with a Network Time Protocol (NTP) server. This ensures that its clock has the same date and time settings as the other servers on your network.

You can configure clock synchronization on your appliance by adding NTP server entries to the `ntp.conf` file from either the configuration utility or the NetScaler command line, or by manually modifying the `ntp.conf` file, and then starting the NTP daemon (NTPD). The clock synchronization configuration does not change if the appliance is restarted, upgraded, or downgraded. However, the configuration does not get propagated to the secondary NetScaler in a high availability setup.

**Note:** If you do not have a local NTP server, you can find a list of public, open access, NTP servers at the official NTP site, <http://www.ntp.org>, under Public Time Servers List. Before configuring your NetScaler to use a public NTP server, be sure to read the Rules of Engagement page (link included on all Public Time Servers pages).

## Setting Up Clock Synchronization by Using the CLI or the Configuration Utility

To configure clock synchronization from the configuration utility or from the CLI, you add NTP servers and then enable NTP synchronization.

### To add an NTP server by using the NetScaler command line

At the NetScaler command prompt, type the following commands to add an NTP server and verify the configuration:

- ♦ `add ntp server (<serverIP> | <serverName>) [-minpoll <positive_integer>][-maxpoll <positive_integer>]`
- ♦ `show ntp server`

#### Example

```
> add ntp server 10.102.29.30 -minpoll 6 -maxpoll
11
Done
> sh ntp server

      NTP Server: xyz.net
      Minimum Poll Interval: 6 (64secs)
      Maximum Poll Interval: 9 (512secs)

      NTP Server: 10.102.29.30
      Minimum Poll Interval: 6 (64secs)
      Maximum Poll Interval: 11 (2048secs)

Done
```

## To modify or remove NTP servers by using the NetScaler command line

- ♦ To modify settings for an NTP server, type the **set ntp server** (<serverIP> | <serverName>) command and the parameters to be changed, with their new values.
- ♦ To remove an NTP server, type **rm ntp server** (<serverIP> | <serverName>)

## Parameters for configuring an NTP server

### serverIP

IP address of the NTP server.

### serverName

Domain name of the NTP server.

### minpoll

Minimum number of seconds after which the NTP server must poll the NTP messages, expressed as a power of 2. Minimum value: 4 ( $2^4=16$  seconds). Maximum value: 17 ( $2^{17}=131072$  seconds). Default: 6 ( $2^6=64$  seconds).

### maxpoll

Maximum number of seconds after which the NTP server must poll the NTP messages, expressed as a power of 2. Minimum value: 4 ( $2^4=16$  seconds). Maximum value: 17 ( $2^{17}=131072$  seconds). Default : 10 ( $2^{10}=1024$  seconds).

## To configure an NTP server by using the configuration utility

1. In the navigation pane, expand **System**, and then click **NTP Servers**.
2. In the details pane, do one of the following:
  - To add a new NTP server, click **Add**.
  - To modify settings for an existing NTP server, select the NTP server, and then click **Open**.
3. In the **Create NTP Server** or **Configure NTP Server** dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring an NTP server” as shown:
  - NTP Server\*—serverIP or serverName (Cannot be changed for an existing NTP server.)
  - Minimum Poll—minpoll
  - Maximum Poll—maxpoll

\* A required parameter
4. Click **Create** or **OK**, and then click **Close**.  
A message appears in the status bar, stating that the NTP server has been configured successfully.

## Starting or Stopping the NTP Daemon

When you enable NTP synchronization, the NetScaler starts the NTP daemon and uses the NTP server entries in the `ntp.conf` file to synchronize its local time setting. If you do not want to synchronize your NetScaler time with the other servers in the network, you can disable NTP synchronization, which stops the NTP daemon (NTPD).

### To enable or disable NTP synchronization by using the NetScaler command line

At the NetScaler command prompt, type one of the following commands:

- ♦ `enable ntp sync`
- ♦ `disable ntp sync`

### To enable or disable NTP synchronization by using the configuration utility

1. In the navigation pane, expand **System**, and then click **NTP Servers**.
2. On the **NTP Servers** page, click **NTP Synchronization - ON** or **NTP Synchronization - OFF**.

## Configuring Clock Synchronization Manually

You can configure clock synchronization manually by logging on to the NetScaler and editing the `ntp.conf` file.

### To enable clock synchronization on your NetScaler by modifying the `ntp.conf` file

1. Log on to the NetScaler command line.
2. Switch to the shell prompt.
3. Copy the `/etc/ntp.conf` file to `/nsconfig/ntp.conf`, unless the `/nsconfig` directory already contains an `ntp.conf` file.
4. Check the `/nsconfig/ntp.conf` file for the following entries and, if they are present, remove them:  
`restrict localhost`  
`restrict 127.0.0.2`
5. Add the IP address for the desired NTP server to the `/nsconfig/ntp.conf` file, beneath the file's `server` and `restrict` entries.

**Note:** For security reasons, there should be a corresponding `restrict` entry for each server entry.



6. If the `/nsconfig` directory does not contain a file named `rc.netscaler`, create the file.
7. Add the following entry to `/nsconfig/rc.netscaler`:  
`/usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ntpd.log &`  
This entry starts the `ntpd` service, checks the `ntp.conf` file, and logs messages in the `/var/log` directory.  
  
This process runs every time the NetScaler is restarted.
8. Reboot the NetScaler to enable clock synchronization.

**Note:**

If you want to start the time synchronization process without restarting the NetScaler, run the following command from the shell prompt:

```
/usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ntpd.log &
```

## Viewing the System Date and Time

To change the system date and time, you must use the shell interface to the underlying FreeBSD OS. However, to view the system date and time, you can use the NetScaler command line or the configuration utility.

### To view the system date and time by using the NetScaler command line

At the NetScaler command prompt, type:

```
show ns config
```

**Example**

```
> show ns config
  NetScaler IP: 10.102.29.170 (mask:
255.255.255.0)
  Number of MappedIP(s): 6
  Node: Standalone

  Global configuration settings:
    HTTP port(s): (none)
    Max connections: 0
    Max requests per connection: 0
    Client IP insertion: DISABLED
    Cookie version: 0
  Persistence Cookie Secure Flag: ENABLED
    Min Path MTU: 576
    Path MTU entry timeout: 10
    FTP Port Range: 0
    CR Port Range: 0
    Timezone: GMT+05:30-
```

```
IST-Asia/Colombo
System Time: Tue Feb 22
16:50:44 2011
Last Config Changed Time: Tue Feb 22
16:48:02 2011
Last Config Saved Time: Tue Feb 22
16:48:19 2011
Done
```

## To view the system date and time by using the configuration utility

1. In the navigation pane, click **System**.
2. In the details pane, select the **System Information** tab.
3. Under **System Information**, view the system date and time.

## Configuring TCP Window Scaling

The TCP window scaling option, which is defined in RFC 1323, increases the TCP receive window size beyond its maximum value of 65,535 bytes. This option is required for efficient transfer of data over long fat networks (LFNs).

A TCP window determines the amount of outstanding (unacknowledged by the recipient) data a sender can send on a particular connection before receiving any acknowledgment from the receiver. The main purpose of the window is flow control.

The window size field in the TCP header is 16 bits, which limits the ability of the sender to advertise a window size larger than 65535 ( $2^{16} - 1$ ). The TCP window scale extension expands the definition of the TCP window by applying a scale factor to the value in the 16 bit window size field of the TCP header. (Although RFC 1323 describes expanding the definition to up to 30 bits, NetScaler window scaling expands the definition of the TCP window to up to 24 bits.) The scale factor is carried in the new TCP window scale field. This field is sent only in a SYN packet (a segment with the SYN bit on)

To fit a larger window size value into the 16-bit field, the sender right shifts the value by the number of bit positions specified by the scale factor. The receiver left shifts the value by the same number of positions. Therefore, the actual window size is equivalent to:

$(2^{\text{scale factor}}) * \text{received window size}$ .

Before configuring window scaling, make sure that:

- ♦ You do not set a high value for the scale factor, because this could have adverse effects on the NetScaler and the network.
- ♦ You have enabled selective acknowledgement (SACK).

- ◆ You do not configure window scaling unless you clearly know why you want to change the window size.
- ◆ Both hosts in the TCP connection send a window scale option during connection establishment. If only one side of a connection sets this option, window scaling is not used for the connection.
- ◆ Each connection for same session is an independent Window Scaling session. For example, when a client's request and the server's response flow through the NetScaler appliance, it is possible to have window scaling between the client and the appliance without window scaling between the appliance and the server.

By default, window scaling is not enabled.

## To configure window scaling by using the NetScaler command line

At the NetScaler command prompt, type the following command to configure window scaling and verify the configuration:

- ◆ `set ns tcpParam [-WS ( ENABLED | DISABLED )] [-WSVal <positive_integer>]`
- ◆ `show ns tcpParam`

```

Example

> set ns tcpParam -WS ENABLED -WSVal 6
Done
> sh ns tcpParam
TCP Parameters

Window Scaling status      : ENABLED
Window Scaling factor      : 6
SACK status                 :
ENABLED
.
.
TCP minimum RTO in millisec: 1000
TCP Slow start increment: 2
Done

```

## Parameters for configuring window scaling

### WSVal

Factor used to calculate new window size. Possible values: 0 to 8. Default: 4.

### WS

Enables or disables window scaling.

## To configure window scaling by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Settings**, click **Configure TCP Parameters**.
3. In the **Configure TCP Parameters** dialog box, under **TCP**, select the **Windows Scaling** check box to enable window scaling.
4. In the **Factor** text box, type a windows scaling factor (for example, **6**). For possible values, see “Parameters for configuring window scaling.”
5. Click **OK**.  
A message appears in the status bar, stating that window scaling has been configured successfully.

## Configuring Selective Acknowledgment

NetScaler appliances support Selective Acknowledgment (SACK), as defined in RFC 2018. Using SACK, the data receiver (either a NetScaler or a client) notifies the sender about all the segments that have been received successfully. As a result, the sender (either a NetScaler or a client) needs to retransmit only those segments that were lost during transmission. This improves the performance of data transmission. SACK is important in long fat networks (LFNs). By default, SACK is disabled.

## To enable Selective Acknowledgment (SACK) by using the NetScaler command line

At the NetScaler command prompt, type the following commands to enable Selective Acknowledgment (SACK) and verify the configuration:

- ◆ `set ns tcpParam [-SACK ( ENABLED | DISABLED )]`
- ◆ `show ns tcpParam`

### Example

```
> set ns tcpParam -SACK ENABLED
Done
> show ns tcpParam
TCP Parameters

Window Scaling status      : ENABLED
Window Scaling factor      : 4
SACK status              : ENABLED
MaxBurst setting          : 6 MSS
Initial cwnd setting       : 4 MSS
TCP Receive Buffer         : 8190 bytes
TCP Delayed-ACK Timer     : 200 millisec
```

```

Down Service Reset status : DISABLED
Nagle's Algorithm : DISABLED
Limited Persist Probes : ENABLED
Maximum out-of-order packets to queue: 64
Done

```

## To enable SACK by using the Configuration Utility

1. In the navigation pane, expand **System**, and click **Settings**.
2. In the details pane, under **Settings**, click **Change TCP Parameters**.
3. In the **Configure TCP Parameters** dialog box, under **TCP**, select the **Selective Acknowledgment** check box, and then click **OK**.  
A message appears in the status bar, stating that SACK has been configured successfully.

## Clearing the Configuration

You have the following three options for clearing your NetScaler configuration.

**Basic level.** Clearing your configuration at the basic level clears all settings except the following:

- ◆ NSIP, MIP(s), and SNIP(s)
- ◆ Network settings (Default Gateway, VLAN, RHI, NTP, and DNS settings)
- ◆ HA node definitions
- ◆ Feature and mode settings
- ◆ Default administrator password (nsroot)

**Extended level.** Clearing your configuration at the extended level clears all settings except the following:

- ◆ NSIP, MIP(s), and SNIP(s)
- ◆ Network settings (Default Gateway, VLAN, RHI, NTP, and DNS settings)
- ◆ HA node definitions

Feature and mode settings revert to their default values.

**Full level.** Clearing your configuration at the full level returns all settings to their factory default values. However, the NSIP and default gateway are not changed, because changing them could cause the NetScaler to lose network connectivity.

## To clear a configuration by using the NetScaler command line

At the NetScaler command prompt, type the following command:

```
clear ns config < ( basic | advanced | full )>
```

#### Example

```
> clear ns config basic
Are you sure you want to clear the configuration(Y/
N)? [N]:Y
Done
```

## Parameters for clearing a configuration

### level

A level representing the extent to which to clear the configuration. Possible values: basic, extended, full.

## To clear a configuration by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Diagnostics**.
2. In the details pane, under **Maintenance**, click **Clear Configuration**.
3. In the **Clear Configuration** dialog box, for **Configuration Level**, select an option (for example, **basic**).
4. Click **Run**. A message appears in the status bar, stating that the configuration has been refreshed successfully.

## Viewing the HTTP Band Statistics

You can view HTTP band statistics to obtain useful information such as:

- ♦ Average request/response band size.
- ♦ The size range to which most requests/responses belong.
- ♦ Contribution of HTTP pages, in a certain size range, to the overall HTTP traffic.

## To view HTTP request and response size statistics by using the NetScaler command line

At the NetScaler command prompt, type:

```
show protocol httpBand -type (REQUEST|RESPONSE)
```

**Example**

```
show protocol httpBand -type REQUEST
show protocol httpBand -type RESPONSE
```

## To view HTTP request and response size statistics by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Settings**, click **HTTP data band statistics**.
3. In the **HTTP Data Band Statistics** dialog box, view the HTTP request and HTTP response size statistics on the **Request** and **Response** tabs, respectively.

You can also modify the band range for HTTP request or response size statistics.

## To modify the band range by using the NetScaler command line

At the NetScaler command prompt, type:

```
set protocol httpBand reqBandSize <value> respBandSize <value>
```

**Example**

```
set protocol httpBand reqBandSize 300 respBandSize
2048
```

## Parameters for modifying the band range for HTTP request or response size statistics

**reqBandSize**

Band size for HTTP request band statistics, in bytes. Minimum value: 50. Maximum value: 2147483647. Default: 100.

**respBandSize**

Band size for HTTP response band statistics, in bytes. Minimum value: 50. Maximum value: 2147483647. Default: 1024.

## To modify the band range by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Settings**, click **HTTP data band Statistics**. Do one or both of the following:
  - To modify the band range of HTTP request statistics, click the **Request** tab, click the **Request** tab, and then click **Configure**. In **Change HTTP Request Band Size** dialog box, enter a value (for example, **300**) in **Request Data Band Size** text field, and then click **OK**.
  - To modify the band range of HTTP response statistics, click the **Response** tab, and then click **Configure**. In **Change HTTP Response Band Size** dialog box, enter a value (for example, **2048**) in **Response Data Band Size** text field, and then click **OK**.
3. Click **Close**.

## Configuring HTTP Profiles

An HTTP profile is a collection of HTTP parameter settings that can be applied to virtual servers and services. An HTTP profile can be reused on multiple virtual servers or services.

You can use built-in HTTP profiles or configure custom profiles. The following table describes the built-in HTTP profiles.

**Table 5-1. Built-in HTTP Profiles**

Built-in profile	Description
nshttp_default_strict_validation	Settings for deployments that require strict validation of HTTP requests and responses.
nshttp_default_profile	The default global HTTP settings for the NetScaler appliance.

## To add an HTTP profile by using the NetScaler command line

At the NetScaler command prompt, type:



- ◆ **add ns httpProfile** name -maxReusePool <value> -dropInvalReqs ( **ENABLED** | **DISABLED** ) -markHttp09Inval ( **ENABLED** | **DISABLED** ) -markConnReqInval ( **ENABLED** | **DISABLED** ) -cmpOnPush ( **ENABLED** | **DISABLED** ) -conMultiplex ( **ENABLED** | **DISABLED** )
- ◆ **sh ns httpProfile**

#### Example

```
add ns httpProfile http_profile1 -maxReusePool 30 -
dropInvalReqs ENABLED -markHttp09Inval ENABLED
-markConnReqInval ENABLED -cmpOnPush ENABLED -
conMultiplex DISABLED
```

## Parameters for adding an HTTP profile

### name (Name)

The name for an HTTP profile. Can be from 1 to 127 characters and must begin with a letter, a number, or the underscore symbol (\_). Additional characters allowed, after the first character, are the hyphen (-), period (.), pound sign (#), space ( ), at sign (@), and equals sign (=).

### maxReusePool (Max Connection in reusepool)

The maximum allowed number of connections, from the NetScaler appliance to a particular server, in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after a peak in the number of connections.

### conMultiplex (Connection Multiplexing)

Reuse existing server connections for multiple client connections. Possible values: ENABLED, DISABLED. Default: ENABLED.

### dropInvalReqs (Drop invalid HTTP requests)

Drop requests or responses in which either the header or the body is invalid. Possible values: ENABLED, DISABLED. Default: DISABLED.

### markHttp09Inval (Mark HTTP/0.9 requests as invalid)

Mark all 0.9 requests as invalid. Possible values: ENABLED, DISABLED. Default: DISABLED.

### markConnReqInval (Mark CONNECT requests as invalid)

Mark all CONNECT requests as invalid. Possible values: ENABLED, DISABLED. Default: DISABLED.

### cmpOnPush (Compression on PUSH packet)

Compress PUSH packets sent by the virtual server to which this profile is bound. Possible values: ENABLED, DISABLED. Default: DISABLED.

## To add an HTTP profile by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Profiles**.
2. In the details pane, on the **HTTP Profiles** tab, click **Add**.
3. In the **Create HTTP Profile** dialog box, set the following parameters:
  - Name\*
  - Max Connection in reusepool
  - Connection Multiplexing
  - Drop invalid HTTP requests
  - Mark HTTP/0.9 requests as invalid
  - Mark CONNECT requests as invalid
  - Compression on PUSH packet

\* A required parameter.
4. Click **Create**. A message appears in the status bar, stating that the HTTP profile has been configured successfully.

## Configuring TCP Profiles

A Transmission Control Protocol (TCP) profile is a collection of TCP parameter settings that can be applied to virtual servers and services. A TCP profile can be reused on multiple virtual servers or services. You can use built-in TCP profiles or configure custom profiles. The following table describes the built-in TCP profiles.

**Table 5-2. Built-in TCP Profiles**

Built-in profile	Description
nstcp_default_tcp_lfp	This profile is useful for long fat pipe networks (WAN) on the client side. Long fat pipe networks have long delay, high bandwidth lines with minimal packet drops.
nstcp_default_tcp_lnp	This profile is useful for long narrow pipe networks (WAN) on the client side. Long narrow pipe networks have considerable packet loss once in a while.

Built-in profile	Description
nstcp_default_tcp_lan	This profile is useful for back-end server connections, where these servers reside on the same LAN as the NetScaler appliance.
nstcp_default_tcp_lfp_thin_stream	This profile is similar to the nstcp_default_tcp_lfp profile; however, the settings are tuned for small size packet flows.
nstcp_default_tcp_lnp_thin_stream	This profile is similar to the nstcp_default_tcp_lnp profile; however, the settings are tuned for small size packet flows.
nstcp_default_tcp_lan_thin_stream	This profile is similar to the nstcp_default_tcp_lan profile; however, the settings are tuned to small size packet flows.
nstcp_default_tcp_interactive_stream	This profile is similar to the nstcp_default_tcp_lan profile; however, it has a reduced delayed ACK timer and ACK on PUSH packet settings.
nstcp_internal_apps	This profile is useful for internal applications on the NetScaler appliance (for example, GSLB sitesyncing). This contains tuned window scaling and SACK options for the desired applications. This profile should not be bound to applications other than internal applications.
nstcp_default_profile	This profile represents the default global TCP settings on the NetScaler appliance.

## To add a TCP profile by using the NetScaler command line

At the NetScaler command prompt, type the following commands to add a TCP profile and verify the configuration:

- ♦ **add ns tcpProfile** name -WS (ENABLED | DISABLED ) -SACK (ENABLED | DISABLED ) -WSVal <value> -nagle (ENABLED | DISABLED ) -ackOnPush (ENABLED | DISABLED ) -maxBurst value -initialCwnd <value> -delayedAck <value> -oooQSize <value> -maxPktPerMss <value> -pktPerRetx <value> -minRTO <value> -slowStartIncr <value>
- ♦ **sh ns tcpProfile**

#### Example

```
add ns tcpProfile tcp_profile1 -WS ENABLED -SACK
ENABLED -WSVal 4 -nagle DISABLED
-ackOnPush ENABLED -maxBurst 10 -initialCwnd 6 -
delayedAck 200 -oooQSize 100
-maxPktPerMss 0 -pktPerRetx 3 -minRTO 200 -
slowStartIncr 3
```

## Parameters for creating a TCP profile

### name (Name\*)

The name for a TCP profile. A TCP profile name can be from 1 to 127 characters and must begin with a letter, a number, or the underscore symbol (\_). Other characters allowed after the first character in a name are the hyphen (-), period (.), pound sign (#), space ( ), at sign (@), and equals sign (=).

### WS (Window Scaling)

Enable or disable window scaling. Possible values: ENABLED, DISABLED. Default: DISABLED.

### WSVal (Factor)

The factor used to calculate the new window size. Possible values: 0 to 8. Default: 4.

### maxBurst (Maximum Burst Limit)

The maximum number of TCP segments allowed in a burst. Minimum value: 2. Maximum value: 10. Default: 6.

### initialCwnd (Initial Congestion Window Size)

The initial maximum upper limit on the number of TCP packets that can be outstanding on the TCP link to the server. Minimum value: 2. Maximum value: 6. Default: 4.

### delayedAck (TCP Delayed ACK Time-out (msec))

The time-out for TCP delayed ACK, in milliseconds. Minimum value: 10. Maximum value: 200. Default: 300.

### oooQSize (Maximum ooo Packet Queue Size)

The maximum size of out-of-order packets queue. Minimum value: 0 0 means infinite). Maximum value: 512. Default: 64.

### maxPktPerMss (Maximum Packets Per MSS)

The maximum number of TCP packets allowed per maximum segment size (MSS). Minimum value: 0. Maximum value: 1460. Default: 0 Means that no maximum is set.)

**pktPerRetx (Maximum Packets per Retransmission)**

The maximum limit on the number of packets that should be retransmitted on receiving a partial ACK. Minimum value: 1. Maximum value: 100. Default: 1.

**minRTO (Minimum RTO (in millisec))**

The minimum round trip to origin (RTO) time, in milliseconds. Minimum value: 10. Maximum value: 64,000. Default: 1,000.

**slowStartIncr (Slow Start Increment)**

The multiplier that determines the rate at which slow start increases the size of the TCP transmission window after each acknowledgement of successful transmission. Minimum value: 1. Maximum value: 100. Default: 2.

**SACK (Selective Acknowledgement)**

Enable or disable selective acknowledgement (SACK). Possible values: ENABLED, DISABLED. Default: DISABLED.

**nagle (Use Nagle's Algorithm)**

Enable or disable the Nagle algorithm on TCP connections. Possible values: ENABLED, DISABLED. Default: DISABLED.

**ackOnPush (Immediate ACK on Receiving Packet with PUSH)**

Send immediate positive acknowledgement (ACK) on receipt of TCP packets when doing Web 2.0 PUSH. Possible values: ENABLED, DISABLED. Default: ENABLED.

## To add a TCP profile by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Profiles**.
2. In the details pane, on the **TCP Profiles** tab, click **Add**.
3. In the **Create TCP Profiles** dialog box, set the following parameters:
  - **Name\***
  - **Window Scaling**
  - **Factor**
  - **Maximum Burst Limit**
  - **Initial Congestion Window Size**
  - **TCP Delayed ACK Time-out (msec)**
  - **Maximum ooo Packet Queue Size**
  - **Maximum Packets Per MSS**
  - **Maximum Packets per Retransmission**
  - **Minimum RTO (in millisec)**
  - **Slow Start Increment**
  - **Selective Acknowledgement**

- Use Nagle's Algorithm
- Immediate ACK on Receiving Packet with PUSH

\* A required parameter.

4. Click **Create**. A message appears in the status bar, stating that the TCP profile has been configured successfully.

## Specifying a TCP Buffer Size

You can set the TCP buffer size, both globally and for individual virtual servers and services, through TCP profiles. The value that you set is the minimum value that is advertised by the NetScaler appliance, and this buffer size is reserved when a client initiates a connection that is associated with an endpoint-application function, such as compression or SSL. The managed application can request a larger buffer, but if it requests a smaller buffer, the request is not honored, and the specified buffer size is used. If the TCP buffer size is set both at the global level and at the entity level (virtual server or service level), the buffer specified at the entity level takes precedence. If the buffer size that you specify for a service is not the same as the buffer size that you specify for the virtual server to which the service is bound, the NetScaler appliance uses the buffer size specified for the virtual server for the client-side connection and the buffer size specified for the service for the server-side connection. However, for optimum results, make sure that the values specified for a virtual server and the services bound to it have the same value. The buffer size that you specify is used only when the connection is associated with endpoint-application functions, such as SSL and compression.

You set the TCP buffer size in a custom, entity-level TCP profile by setting the `bufferSize` parameter for the profile. To apply the buffer size setting specified in a custom, entity-level profile, you bind the profile to the virtual server or service. You set the global TCP buffer size by setting the `bufferSize` parameter in the global TCP profile `nstcp_default_profile`. You do not bind `nstcp_default_profile` to an entity. The settings in `nstcp_default_profile` are automatically applied globally.

**Note:** A high TCP buffer value could limit the number of connections that can be made to the NetScaler appliance. Additionally, the global TCP parameter `recvBuffSize`, which was set by the use of the `set ns tcpParam` command, has been deprecated. You can now specify the buffer size only through TCP profiles.

## To set the TCP buffer size in an entity-level TCP profile by using the NetScaler command line

At the NetScaler command prompt, type the following commands to set the TCP buffer size in a TCP profile and verify the configuration:

- ♦ `set ns tcpProfile <name> -bufferSize <positive_integer>`
- ♦ `show ns tcpProfile <name>`

**Example**

```
> set ns tcpProfile profile1 -bufferSize 12000
Done
> show ns tcpProfile profile1
      Name      : profile1
      Window Scaling status      : DISABLED
      Window Scaling factor      : 4
      .
      .
      .
      TCP Buffer Size      : 12000 bytes
      Reference count: 0

Done
>
```

## To set the TCP buffer size in the global TCP profile by using the NetScaler command line

At the NetScaler command prompt, type the following commands to set the TCP buffer size in the global TCP profile and verify the configuration:

- ◆ **set ns tcpProfile nstcp\_default\_profile -bufferSize <positive\_integer>**
- ◆ **show ns tcpProfile nstcp\_default\_profile**

**Example**

```
> set ns tcpProfile nstcp_default_profile -
bufferSize 12000
Done
> show ns tcpProfile nstcp_default_profile
      Name      : nstcp_default_profile
      Window Scaling status      : DISABLED
      Window Scaling factor      : 4
      .
      .
      .
      TCP Buffer Size      : 12000 bytes
      Reference count: 200

Done
>
```

## Parameters for setting the TCP buffer size in a TCP profile

**name**

Name of the TCP profile. Maximum length: 127 characters.

**bufferSize**

TCP buffer size in bytes. Maximum value: 4194304. Minimum value: 8190. Default: 8190.

## To set the TCP buffer size in a TCP profile by using the NetScaler configuration utility

1. In the navigation pane, expand **System**, and then click **Profiles**.
2. In the details pane, click the **TCP Profiles** tab, and then do one of the following:
  - To create a custom, entity-level TCP profile, click **Add** and, in the **Create TCP Profile** dialog box, type a name for the new profile.
  - To set the TCP buffer size for an existing TCP profile, click the name of the TCP profile, and then click **Open**. If you want to set the TCP buffer size in the global TCP profile, click `nstcp_default_profile`.
3. In the **Create TCP Profile** or **Configure TCP Profile** dialog box, in the **TCP Buffer Size (Bytes)** box, type the number of bytes to specify as the minimum TCP buffer size.
4. Click **Create** or **OK**.

## Optimizing the TCP Maximum Segment Size for a Virtual Server Configuration

You can specify the Maximum Segment Size (MSS) that the Citrix® NetScaler® appliance advertises to a client when the client initiates a connection to a virtual server on the appliance. You can configure the MSS for the virtual servers configured on the appliance in two ways:

- ♦ You can set the MSS for each virtual server to a value of your choice in a TCP profile.
- ♦ You can set the `learnVsvrMSS` global TCP parameter to `ENABLED` to enable MSS learning for all the virtual servers configured on the appliance.

If you know the optimal MSS value for a given virtual server, you can specify the MSS in a TCP profile and bind the profile to the virtual server. When a client initiates a connection with the virtual server, the NetScaler appliance advertises the specified MSS value to the client. However, if the appliance is also configured to learn the optimum MSS value from bound services (as described in the following section), the learned MSS value takes precedence, and the value specified in the TCP profile is used only until



the appliance learns the optimum MSS value. The appliance uses the learned MSS value until the appliance is restarted. If the appliance is restarted, the appliance defaults to the MSS value specified in the virtual server's TCP profile until it learns the MSS value again.

## Specifying the MSS Value in a TCP Profile

If you know the optimal MSS value for a given virtual server, you can specify the MSS in a TCP profile and bind the profile to the virtual server. When a client initiates a connection with the virtual server, the NetScaler appliance advertises the specified MSS value to the client.

### To specify the MSS value in a TCP profile by using the NetScaler command-line

At the NetScaler command prompt, type the following commands to specify the MSS value in a TCP profile and verify the configuration:

- ◆ **add ns tcpProfile** <name> **-mss** <positive\_integer>
- ◆ **show ns tcpProfile**

```
> add ns tcpProfile tcp_prof1 -mss 1000
Done
> show ns tcpProfile tcp_prof1
Name      : tcp_prof1
Window Scaling status      : DISABLED
Window Scaling factor     : 4
SACK status                : DISABLED
MSS                    : 1000
MaxBurst setting          : 6 MSS
Initial cwnd setting      : 4 MSS
.
.
.
Done
>
```

### Parameters for specifying the MSS value in a TCP profile

#### name

The name of the TCP profile.

#### mss

The maximum number of octets to allow in a TCP data segment.

### To specify the MSS value in a TCP profile by using the NetScaler configuration utility

1. In the navigation pane, expand **System**, and then click **Profiles**.
2. In the details pane, do one of the following:

- To create a TCP profile, click **Add**.
  - To specify the MSS in an existing TCP profile, click the name of the profile, and then click **Open**.
3. In the **Create TCP Profile** or **Configure TCP Profile** dialog box, specify values for the following parameters, which correspond to the parameters described in "Parameters for specifying the MSS value in a TCP profile" as shown:
    - **Name\***—name (cannot be changed for an existing TCP profile)
    - **MSS\***—mss

\* A required parameter
  4. Click **Create** or **OK**.

## Configuring the NetScaler to Learn the MSS Value from Bound Services

If you set the global TCP parameter `learnVsvrMSS` to `ENABLED`, the NetScaler appliance learns the most frequently used MSS value for each configured virtual server. When a client connects to a virtual server, the appliance advertises to the client the MSS value that is optimum for that virtual server. The optimum value is the MSS of the service or subset of bound services that are most frequently selected during load balancing. Consequently, each virtual server configuration uses its own MSS value. This enhancement enables the appliance to optimize the consumption of system resources.

The default value of the `learnVsvrMSS` parameter is `DISABLED`. When enabled, MSS learning is applicable only to virtual servers of type TCP, HTTP, and FTP.

### To configure the NetScaler to learn the MSS for a virtual server by using the NetScaler command-line

At the NetScaler command prompt, type the following commands to configure the NetScaler to learn the MSS for a virtual server and verify the configuration:

- ♦ `set ns tcpParam -learnVsvrMSS (ENABLED|DISABLED)`
- ♦ `show ns tcpParam`

#### Example

```
> set ns tcpParam -learnVsvrMSS ENABLED
Done
> show ns tcpParam
TCP Parameters

Window Scaling status      : DISABLED
Window Scaling factor      : 4
SACK status                 : DISABLED
Learn MSS for VServer    : ENABLED
.
.
.
```



## Parameters for configuring the NetScaler to learn the MSS for a virtual server

### learnVsvrMSS

Enable or disable MSS learning for virtual servers. Possible values: `ENABLED`, `DISABLED`. Default: `DISABLED`.

## To configure the NetScaler to learn the MSS for a virtual server by using the NetScaler configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, click **Change TCP parameters**.
3. In the **Configure TCP Parameters** dialog box, select the **Learn MSS** check box.



---

## Chapter 6

# Web Interface

### Topics:

- [How Web Interface Works](#)
- [Prerequisites](#)
- [Installing the Web Interface](#)
- [Configuring the Web Interface](#)

The Web Interface on Citrix® NetScaler® appliances is based on Java Server Pages (JSP) technology and provides access to Citrix® XenApp™ and Citrix® XenDesktop® applications. Users access resources through a standard Web browser or by using the Citrix XenApp plug-in.

The Web Interface runs as a service on port 8080 on the NetScaler appliance. To create Web Interface sites, Java is executed on Apache Tomcat Web server version 6.0.26 on the NetScaler appliance. The Web Interface sites provide user access to the XenApp and XenDesktop resources, which include applications, content, and desktops.

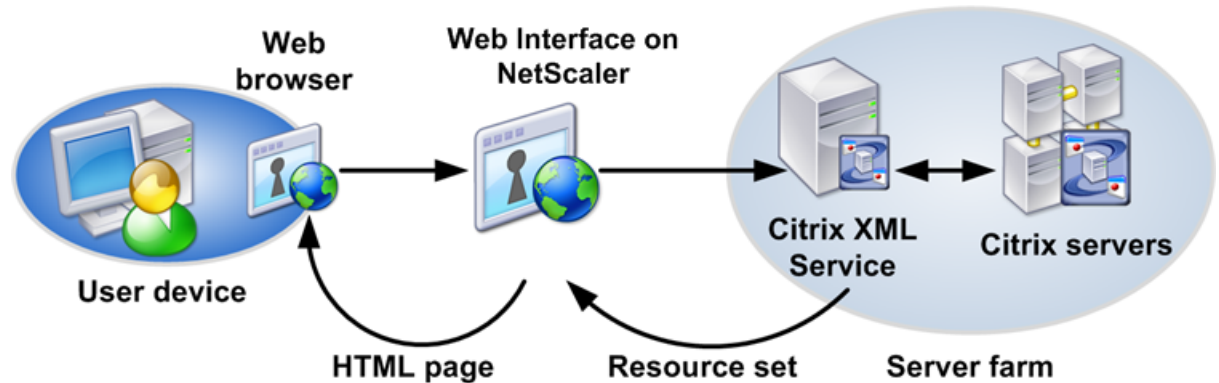
**Note:** This feature is supported only on NetScaler nCore builds.

The Web Interface installation includes installing the Web Interface tar file and JRE tar file on the NetScaler appliance. To configure the Web Interface, you create a Web Interface site and bind one or more XenApp or XenDesktop farms to it.

## How Web Interface Works

The following figure illustrates a basic Web interface session.

**Figure 6-1. A Basic Web Interface Session**



Following is a typical set of interactions among a user device, a NetScaler running the Web interface, and a server farm.

1. A user authenticates to the Web interface through a Web browser or by using the XenApp plug-in.
2. The Web interface reads the user's credentials and forwards the information to the Citrix XML Service running on servers in the server farm.
3. The Citrix XML Service on the designated server retrieves from the servers a list of resources that the user can access. These resources constitute the user's resource set and are retrieved from the Independent Management Architecture (IMA) system.
4. The Citrix XML Service then returns the user's resource set to the Web interface running on the NetScaler.
5. The user clicks an icon that represents a resource on the HTML page.
6. The Web interface queries the Citrix XML Service for the least busy server.
7. The Citrix XML Service returns the address of this server to the Web interface.
8. The Web interface sends the connection information to the Web browser.
9. The Web browser initiates a session with the server.

## Prerequisites

The following prerequisites are required before you begin installing and configuring the Web interface.

- ♦ XenApp or XenDesktop farms are set up and running in your environment. For more information about XenApp, see the XenApp documentation at <http://>

[edocs.citrix.com/](http://edocs.citrix.com/). For more information about XenDesktop, see the XenDesktop farms documentation at <http://edocs.citrix.com/>.

- ◆ Conceptual knowledge of the Web interface. For more information about Web interface running on a server, see the Web interface documentation at <http://edocs.citrix.com/>.

## Installing the Web Interface

To install the Web interface, you need to install the following files:

- ◆ **Web interface tar file.** A setup file for installing the Web interface on the NetScaler. This tar file also includes Apache Tomcat Web server version 6.0.26. The file name has the following format: `nswi-<version number>.tgz` (for example, `nswi-1.1.tgz`).
- ◆ **JRE tar file.** This is Diablo Latte JRE version 1.6.0-7 for 64-bit FreeBSD 6.x/amd64 platform. To download the JRE tarball, see the FreeBSD Foundation Web site at <http://www.freebsdoundation.org/downloads/java.shtml>.

Copy the tar files to a local workstation or to the `/var` directory of the NetScaler appliance.

These files install all the Web interface components and JRE on the NetScaler hard drive and configure automatic startup of the Tomcat Web server with Web interface at the NetScaler appliance startup time. Both tar files are internally expanded in the `/var/wi` directory on the hard drive.

## To install the Web interface and JRE tar files by using the NetScaler command line

At the NetScaler command prompt, type:

```
install wi package -wi <URL> -jre <URL>
```

### Example

```
install wi package -wi sftp://  
username:password@10.102.29.12/var/nswi-1.1.tgz -  
jre ftp://username:password@10.102.29.14/tmp/  
diablojre- freebsd6.amd64.1.6.0.07.02.tbz  
install wi package -wi ftp://  
username:password@10.102.29.15/var/nswi-1.1.tgz -  
jre file:///var/diablo-  
jrefreebsd6.amd64.1.6.0.07.02.tbz
```

## Parameters for installing the Web interface and JRE tar files

### Web Interface tar file path

Complete path to the Web interface tar file.

### JRE tar file path

Complete path to the JRE tar file.

## To install the Web interface and JRE tar files by using the configuration utility

1. In the navigation pane, click **Web Interface**.
2. In the details pane, under **Getting Started**, click **Install Web Interface**.
3. In the **Install Web Interface** dialog box, in the **Web Interface tar file path** text box, type the complete path to the Web interface tar file. You can also use the **browse** button to locate the file on your local system or the NetScaler hard drive.
4. In the **JRE tar file path** text box, type the complete path to the JRE tar file. You can also use the **browse** button to locate the file on your local system or the NetScaler hard drive.
5. Click **Install**.

## Configuring the Web Interface

To configure the Web interface, you create a Web interface site and bind one or more XenApp or XenDesktop farms to it. You then configure the Web interface to work behind an HTTP or an HTTPS virtual server or Citrix Access Gateway™.

The following access methods are available for setting up Web interface sites:

- ♦ **Direct Mode.** You create an HTTP or an HTTPS virtual server on the NetScaler appliance and bind the Web interface service, running on port 8080 of the NetScaler appliance, to the virtual server. Clients on the LAN use the virtual server IP address to access the Web interface. When using this access method, the URL format for the Web interface site is as follows:

```
<HTTP or HTTPS>://<HTTP or HTTPS vserver IP address>:<vserver port number>/<Web Interface site path>
```

- ♦ **Gateway Direct Mode.** You associate the Web interface site with Access Gateway. Remote clients use the Access Gateway URL to access the Web interface site. With this access method, the URL format for the Web interface site is as follows:



---

HTTPS://<Access Gateway URL>/<Web Interface site path>

## Parameters for configuring Web interface sites

### Site Type

Type of site. Possible values: XenApp/XenDesktop Web Site (configures the Web interface site for access by a Web browser); XenApp/XenDesktop Services Site (configures the Web interface site for access by the XenApp plug-in). Default: XenApp/XenDesktop Web Site.

### Site Path

Path to the Web interface site. This parameter is required. Type a site path or select one of the following:

- ◆ /Citrix/XenApp/
- ◆ /Citrix/DesktopWeb/
- ◆ /Citrix/PNAgent/

### Published Resource Type

Method for accessing the published XenApp and XenDesktop resources. Possible values: Online (allows applications to be launched on the XenApp and XenDesktop servers); Offline (allows streaming of applications to the client); DualMode (allows both modes). Default: Online.

### Kiosk Mode

Specifies whether user settings should be persistent or last only for the lifetime of the session. When Kiosk mode is enabled, user settings do not persist from one session to another. Possible values: ON, OFF. Default value: OFF.

### Direct Mode

The Web interface is accessed through an HTTP or an HTTPS loopback load balancing virtual server.

### Virtual Server

Lists existing loopback load balancing virtual servers and an option to create a new one.

### Protocol

The type of services to which the virtual server distributes requests. Possible values: HTTP, HTTPS. Default: HTTP.

### IP Address

IP address of the virtual server. Can be an IPv4 or IPv6 address.

**Port**

Port on which the virtual server listens for client connections. Possible values: from 0 through 65535.

**Gateway Direct Mode**

The Web interface is accessed through a configured Access Gateway.

**Authentication Point**

Authentication point to be used for the site. Possible values: Web interface, AccessGateway. Default: AccessGateway.

**Access Gateway URL**

URL of the Access Gateway.

**Add DNS Entry**

Specifies whether to add DNS address record to resolve the specified Access Gateway URL. Possible values: ON, OFF. Default: ON.

**Trust SSL Certificate**

Specifies whether the Web interface site trusts certificates signed by a non-trusted CA. Possible values: ON, OFF. Default: ON.

**STA Server URL**

URL of the Secure Ticket Authority (STA) server.

**STA Server URL (2)**

URL of the second STA server.

**Session Reliability**

Specifies whether to use session reliability through the Access Gateway. Possible values: ON, OFF. Default: OFF.

**Use Two STA Servers**

Specifies whether the Web interface requests tickets from two separate gateway Secure Ticket Authorities when a resource is accessed. Possible values: ON, OFF. Default: OFF.

**Name**

Name of a XenApp or XenDesktop farm. Any name can be used as a logical representation of a XenApp or XenDesktop farm. The name must not exceed 127 characters.

**XML Service Addresses**

Comma-separated IP addresses or host names of either XenApp or XenDesktop servers providing XML services.

**XML Service Port**

Port number to use for contacting the XML service. Default: 80.

**Transport**

Transport protocol to use for the XML service. Possible values: HTTP, HTTPS. Default: HTTP.

**Load balance**

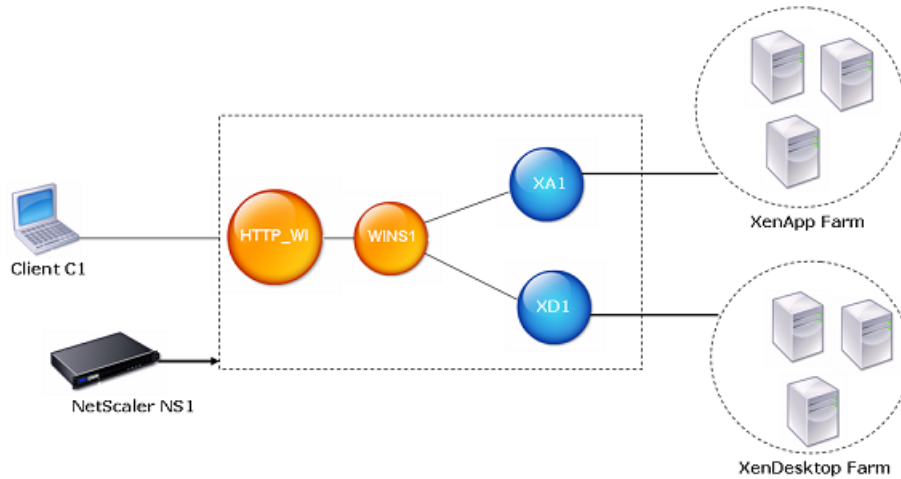
Specifies whether to use all the XML servers (load balance mode) or only one (failover mode). Possible values: ON (load balance mode), OFF (failover mode). Default: ON.

## Configuring a Web Interface Site for LAN Users Using HTTP

In this scenario, user and the Web interface setup are on the same enterprise LAN. The enterprise has both a XenApp and a XenDesktop farm. Users access the Web interface by using an HTTP vserver. The Web interface exposes its own login page for authentication. The vserver IP address is used to access the Web interface.

The following figure illustrates the Web interface running on the NetScaler appliance NS1. A Web interface site WINS1 is created and a XenApp farm XA1 and a XenDesktop farm XD1 are bound to it. An HTTP vserver HTTP\_WI is also created. Client C1 uses the IP address of the HTTP\_WI vserver to access the WINS1 site.

**Figure 6-2. A Web Interface Site Configured for LAN Users Using HTTP**



### To configure a Web interface site for LAN users using HTTP by using the configuration utility

1. In the navigation pane, click **Web Interface**.
2. In the details pane, click **Web Interface Wizard**.
3. On the wizard **Introduction** page, click **Next**.
4. On the wizard **Configure Web Interface Site** page, specify the values for the following parameters, which correspond to parameters described in [Parameters for configuring Web interface sites](#) on page 153 as shown:

- **Site Path\*** (You cannot change the name of an existing Web interface site.)
- **Site Type**
- **Published Resource Type**
- **Kiosk Mode**
- 
- 
- 
- 

\* A required parameter.

5. Select **Direct Mode** and specify values for the following parameters, which correspond to parameters described in [Parameters for configuring Web interface sites](#) on page 153 as shown:
  - **Virtual Server**
  - **Protocol** (select HTTPS)
  - **IP Address**
  - **Port**

**Note:**

When you create the HTTPS vserver by using the configuration utility, the configuration utility automatically creates a service, which logically represents the Web interface service running on the NetScaler appliance, and binds the service to the HTTPS virtual server.

For more information about services and virtual servers, see the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.

6. Click **Next**.
7. On the wizard's **Configure XenApp/XenDesktop Farm** page, do one of the following:
  - To add a XenApp or XenDesktop farm, click **Add**.
  - To modify an existing XenApp or XenDesktop farm, select the farm, and then click **Open**.
8. In the **Create XenApp/XenDesktop Farm** or **Configure XenApp/XenDesktop Farm** dialog box, specify values for the following parameters, which correspond to parameters described in [Parameters for configuring Web interface sites](#) on page 153 as shown:
  - **Name\*** (You cannot change the name of an existing XenApp or XenDesktop farm.)
  - **XML Service Addresses\***
  - **XML Service Port**
  - **Transport**
  - **Load Balance**

\* A required parameter.
9. Click **Next**, and then click **Finish**.
10. Verify that the Web interface site you configured is correct by selecting the site and viewing the **Details** section at the bottom of the pane. To view the Web interface site, in the navigation pane, expand **System**, expand **Web Interface**, and then click **Sites**.

## To configure a Web interface site for LAN users using HTTP by using the command line

1. Add a Web interface site. Set **Direct** or **Alternate** or **Translated** for the `defaultAccessMethod` parameter. At the NetScaler command prompt, type:

```
add wi site <sitePath> -siteType ( XenAppWeb | XenAppServices ) -
publishedResourceType ( Online | Offline | DualMode ) -kioskMode ( ON | OFF)
```

### Example

```
add wi site WINS1 -siteType XenAppWeb -publishedResourceType
Online -kioskMode ON
```

2. Bind XenApp or XenDesktop farms to the Web interface site. At the NetScaler command prompt, type:

```
bind wi site <sitePath> <farmName> <xmlServerAddresses> -xmlPort <value> -
transport ( HTTP | HTTPS) -loadBalance ( ON | OFF )
```

### Example

```
bind wi site WINS1 XA1 10.102.46.6 -xmlPort 80 -transport HTTP
-LoadBalance OFF
bind wi site WINS1 XD1 10.102.46.50 -xmlPort 80 -transport
HTTP -LoadBalance OFF
```

3. Create a service that is a logical representation of the Web interface service running on the NetScaler appliance. At the NetScaler command prompt, type:

```
add service <name> <IP address> <serviceType> <port>
```

### Example

```
add service WI_Loopback_Service 127.0.0.1 HTTP 8080
```

For more information, see the “Load Balancing” chapter of the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.

4. Add an HTTP vserver. At the NetScaler command prompt, type:

```
add lb vserver <virtualServerName> <protocol> <IPAddress> <port>
```

### Example

```
add lb vserver HTTP_WI HTTP 10.102.29.5 80
```

For more information, see the “Load Balancing” chapter of the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.

5. Bind the Web interface service to the HTTP vserver. At the NetScaler command prompt, type:

```
bind lb vserver <virtualServerName> <serviceName>
```

### Example

```
bind lb vserver HTTP_WI WI_Loopback_Service
```

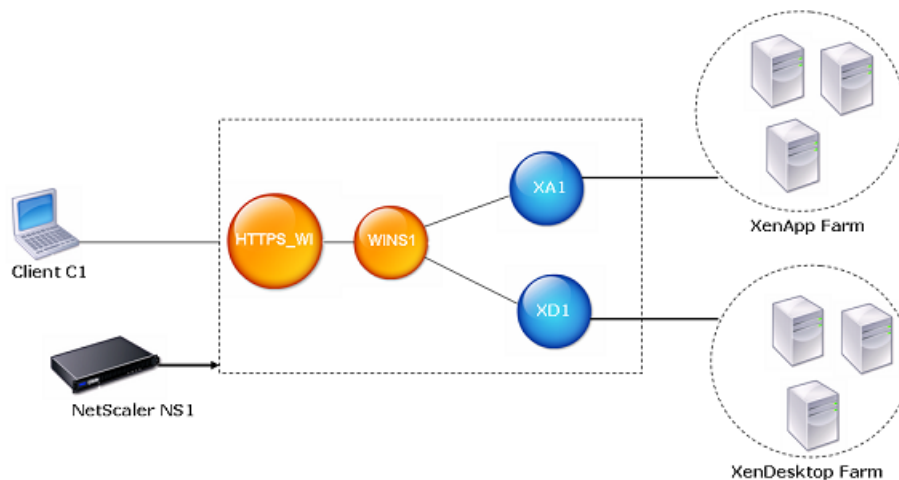
For more information, see the “Load Balancing” chapter of the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.

## Configuring a Web Interface Site for LAN Users Using HTTPS

In this scenario, user accounts and the Web interface setup are on the same enterprise LAN. Users access the Web interface by using an SSL-based (HTTPS) vserver. The Web interface exposes its own login page for authentication. SSL offloading is done by this vserver on the NetScaler. The vserver IP address is used to access the Web interface instead of the NetScaler IP address (NSIP).

The following figure illustrates the Web interface running on the NetScaler appliance NS1. A Web interface site WINS1 is created and a XenApp farm XA1 and a XenDesktop farm XD1 are bound to it. An HTTPS vserver HTTPS\_WI is also created. Client C1 uses the IP address of the HTTPS\_WI vserver to access the WINS1 site.

**Figure 6-3. A Web Interface Site Configured for LAN Users Using HTTPS**



### To configure a Web interface site for LAN users using HTTPS by using the configuration utility

1. In the navigation pane, click **Web Interface**.
2. In the details pane, click **Web Interface Wizard**.
3. On the wizard **Introduction** page, click **Next**.
4. On the wizard **Configure Web Interface Site** page, specify the values for the following parameters, which correspond to parameters described in [Parameters for configuring Web interface sites](#) on page 153 as shown:

- **Site Path\*** (You cannot change the name of an existing Web interface site.)
- **Site Type**
- **Published Resource Type**
- **Kiosk Mode**
- 
- 
- 
- 

\* A required parameter.

5. Select **Direct Mode** and specify values for the following parameters, which correspond to parameters described in [Parameters for configuring Web interface sites](#) on page 153 as shown:
  - **Virtual Server**
  - **Protocol** (select HTTPS)
  - **IP Address**
  - **Port**

**Note:**

When you create the HTTPS vserver by using the configuration utility, the configuration utility automatically creates a service, which logically represents the Web interface service running on the NetScaler appliance, and binds the service to the HTTPS virtual server.

For more information about services and virtual servers, see the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.

6. Click **Next**.
7. On the wizard's **Specify a server Certificate** page, you create or specify an existing SSL certificate-key pair. The SSL certificate-key pair is automatically bound to the HTTPS vserver.

For more information, see “Binding an SSL Certificate Key Pair to the Virtual Server” in the “Secure Sockets Layer (SSL) Acceleration” chapter of the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.
8. Click **Next**.
9. On the wizard's **Configure XenApp/XenDesktop Farm** page, do one of the following:
  - To add a XenApp or XenDesktop farm, click **Add**.
  - To modify an existing XenApp or XenDesktop farm, select the farm, and then click **Open**.



10. In the **Create XenApp/XenDesktop Farm** or **Configure XenApp/XenDesktop Farm** dialog box, specify values for the following parameters, which correspond to parameters described in [Parameters for configuring Web interface sites](#) on page 153 as shown:
  - **Name\*** (You cannot change the name of an existing XenApp or XenDesktop farm.)
  - **XML Service Addresses\***
  - **XML Service Port**
  - **Transport**
  - **Load Balance**

\* A required parameter.
11. Click **Next**, and then click **Finish**.
12. Verify that the Web interface site you configured is correct by selecting the site and viewing the **Details** section at the bottom of the pane. To view the Web interface site, in the navigation pane, expand **System**, expand **Web Interface**, and then click **Sites**.

## To configure a Web interface site for LAN users using HTTPS by using the command line

1. Add a Web interface site. Set **Direct** or **Alternate** or **Translated** for the `defaultAccessMethod` parameter. At the NetScaler command prompt, type:
 

```
add wi site <sitePath> -siteType ( XenAppWeb | XenAppServices ) -
publishedResourceType ( Online | Offline | DualMode ) -kioskMode ( ON | OFF)
```

### Example

```
add wi site WINS1 -siteType XenAppWeb -publishedResourceType
Online -kioskMode ON
```

2. Bind XenApp or XenDesktop farms to the Web interface site. At the NetScaler command prompt, type:
 

```
bind wi site <sitePath> <farmName> <xmlServerAddresses> -xmlPort <value> -
transport ( HTTP | HTTPS ) -loadBalance ( ON | OFF )
```

### Example

```
bind wi site WINS1 XA1 10.102.46.6 -xmlPort 80 -transport HTTP
-LoadBalance OFF
bind wi site WINS1 XD1 10.102.46.50 -xmlPort 80 -transport
HTTP -LoadBalance OFF
```

3. Create a service that is a logical representation of the Web interface service running on the NetScaler appliance. At the NetScaler command prompt, type:
 

```
add service <name> <IPAddress> <serviceType> <port>
```

### Example

```
add service WI_Loopback_Service 127.0.0.1 HTTP 8080
```

For more information, see the “Load Balancing” chapter of the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.

4. Add an HTTPS vserver. At the NetScaler command prompt, type:

```
add lb vserver <virtualServerName> <protocol> <IPAddress> <port>
```

**Example**

```
add lb vserver HTTPS_WI SSL 10.102.29.3 443
```

For more information, see “Adding an SSL-Based Virtual Server” in the “Secure Sockets Layer (SSL) Acceleration” chapter of the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.

5. Bind the Web interface service to the HTTPS vserver. At the NetScaler command prompt, type:

```
bind lb vserver <virtualServerName> <serviceName>
```

**Example**

```
bind lb vserver HTTPS_WI WI_Loopback_Service
```

For more information, see “Binding Services to the Virtual Server” in the “Secure Sockets Layer (SSL) Acceleration” chapter of the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.

6. Create an SSL certificate key pair. At the NetScaler command prompt, type:

```
add ssl certkey <certificate-KeyPairName> -cert <certificateFileName> -key <privateKeyFileName>
```

**Example**

```
add ssl certkey SSL-Certkey-1 -cert /nsconfig/ssl/test1.cer -key /nsconfig/ssl/test1
```

For more information, see “Adding a Certificate Key Pair” in the “Secure Sockets Layer (SSL) Acceleration” chapter of the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.

7. Bind the SSL certificate key pair to the HTTPS vserver. At the NetScaler command prompt, type:

```
bind ssl vserver <vserverName> -certkeyName <certificate- KeyPairName>
```

**Example**

```
bind ssl vserver HTTPS_WI -certkeyName SSL-Certkey-1
```

For more information, see “Binding an SSL Certificate Key Pair to the Virtual Server” in the “Secure Sockets Layer (SSL) Acceleration” chapter of the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.

8. Add a rewrite action. At the NetScaler command prompt, type:

```
add rewrite action <name> <type> <target> [<stringBuilderExpr>] [(-pattern <expression>)]
```

**Example**

```
add rewrite action Replace_HTTP_to_HTTPS INSERT_AFTER "HTTP.RES.HEADER(\"Location\").Value(0).Prefix(4) " "s\""
```

For more information, see “Configuring a Rewrite Action” in the “Rewrite” chapter of the *Citrix NetScaler AppExpert Guide* at <http://support.citrix.com/article/CTX128682>.

9. Create a rewrite policy and bind the rewrite action to it. At the NetScaler command prompt, type:

```
add rewrite policy <name> <expression> <rewriteAction>
```

#### Example

```
add rewrite policy rewrite_location "HTTP.RES.STATUS == 302 &&
HTTP.RES.HEADER(\"Location\").Value(0).startswith(\"http:\")"
Replace_HTTP_to_HTTPS
```

For more information, see “Configuring a Rewrite Policy” in the “Rewrite” chapter of the *Citrix NetScaler AppExpert Guide* at <http://support.citrix.com/article/CTX128682>.

10. Bind the rewrite policy to the HTTPS vserver. At the NetScaler command prompt, type:

```
bind lb vserver <VserverName> -policyname <rewritePolicyName> -priority <value>
-type response
```

#### Example

```
bind lb vserver HTTPS_WI -policyname rewrite_location -
priority 10 -type response
```

For more information, see “Binding a Rewrite Policy” in the “Rewrite” chapter of the *Citrix NetScaler AppExpert Guide* at <http://support.citrix.com/article/CTX128682>.

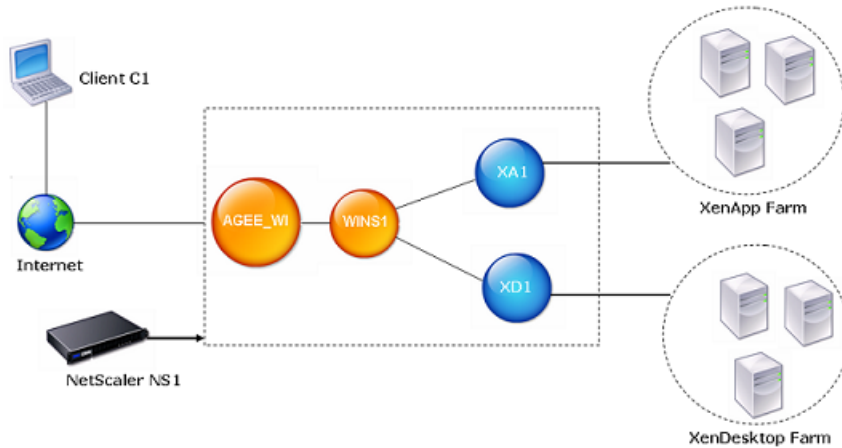
## Configuring a Web Interface Site for Remote Users Using AGEE

In this scenario, user accounts and the Web interface setup are on different networks. Users access a Web interface site by using Access Gateway Enterprise Edition (AGEE) URL. SmartAccess is automatically enabled.

The following figure illustrates the Web interface running on the NetScaler appliance NS1. A Web interface site WINS1 is created and a XenApp farm XA1 and a XenDesktop XD1 are bound to it. An AGEE VPN vserver AGEE\_WI is also configured. The client uses the AGEE URL of the AGEE\_WI to access the WINS1 site.

For more information about configuring AGEE, see the AGEE documentation at <http://edocs.citrix.com/>.

**Figure 6-4. A Web Interface Site Configured for Remote Users Using AGEE**



## To configure a Web interface site for remote users using AGEE by using the configuration utility

1. In the navigation pane, click **Web Interface**.
2. In the details pane, click **Web Interface Wizard**.
3. On the wizard **Introduction** page, click **Next**.
4. On the wizard **Configure Web Interface Site** page, specify the values for the following parameters, which correspond to parameters described in [Parameters for configuring Web interface sites](#) on page 153 as shown:
  - **Site Path\*** (You cannot change the name of an existing Web interface site.)
  - **Site Type**
  - **Published Resource Type**
  - **Kiosk Mode**
  - 
  - 
  - 
  -

\* A required parameter.

5. Select **Gateway Direct Mode** and specify values for the following parameters, which correspond to parameters described in [Parameters for configuring Web interface sites](#) on page 153 as shown:

- Authentication Point
  - Access Gateway URL
  - Add DNS Entry
  - Trust SSL Certificate
  - STA Server URL
  - STA Server URL (2)
  - Session Reliability
  - Use two STA Servers
6. Click **Next**.
  7. On the wizard's **Configure XenApp/XenDesktop Farm** page, do one of the following:
    - To add a XenApp or XenDesktop farm, click **Add**.
    - To modify an existing XenApp or XenDesktop farm, select the farm, and then click **Open**.
  8. In the **Create XenApp/XenDesktop Farm** or **Configure XenApp/XenDesktop Farm** dialog box, specify values for the following parameters, which correspond to parameters described in [Parameters for configuring Web interface sites](#) on page 153 as shown:
    - **Name\*** (You cannot change the name of an existing XenApp or XenDesktop farm.)
    - **XML Service Addresses\***
    - **XML Service Port**
    - **Transport**
    - **Load Balance**

\* A required parameter.
  9. Click **Next**, and then click **Finish**.
  10. Verify that the Web interface site you configured is correct by selecting the site and viewing the **Details** section at the bottom of the pane. To view the Web interface site, in the navigation pane, expand **System**, expand **Web Interface**, and then click **Sites**.

## To configure a Web interface site for remote users using AGEE by using the command line

1. Add a Web interface site. Set **GatewayDirect** or **GatewayAlternate** or **GatewayTranslated** for the defaultAccessMethod parameter. At the NetScaler command prompt, type:
 

```
add wi site <sitePath> <agURL> <staURL> -sessionReliability ( ON | OFF ) -
useTwoTickets ( ON | OFF ) -secondSTAURL <string> -authenticationPoint
( WebInterface | AccessGateway ) -siteType ( XenAppWeb | XenAppServices ) -
publishedResourceType ( Online | Offline | DualMode ) -kioskMode ( ON | OFF )
```

**Example**

```
add wi site WINS1 https://ag.mycompany.com http://
ag.staserver.com -sessionReliability OFF -authenticationPoint
AccessGateway -siteType XenAppWeb -publishedResourceType
Online -kioskMode ON
```

2. Bind XenApp or XenDesktop farms to the Web interface site. At the NetScaler command prompt, type:

```
bind wi site <sitePath> <farmName> <xmlServerAddresses> -xmlPort <value> -
transport ( HTTP | HTTPS) -loadBalance ( ON | OFF )
```

**Example**

```
bind wi site WINS1 XA1 10.102.46.6 -xmlPort 80 -transport HTTP
-LoadBalance OFF
bind wi site WINS1 XD1 10.102.46.50 -xmlPort 80 -transport
HTTP -LoadBalance OFF
```

---

# Chapter 7

## AppFlow

### Topics:

- [How AppFlow Works](#)
- [Configuring the AppFlow Feature](#)

The Citrix® NetScaler® appliance is a central point of control for all application traffic in the data center. It collects flow and user-session level information valuable for application performance monitoring, analytics, and business intelligence applications. AppFlow transmits the information by using the Internet Protocol Flow Information eXport (IPFIX) format, which is an open Internet Engineering Task Force (IETF) standard defined in RFC 5101. IPFIX (the standardized version of Cisco's NetFlow) is widely used to monitor network flow information. AppFlow defines new Information Elements to represent application-level information.

Using UDP as the transport protocol, AppFlow transmits the collected data, called *flow records*, to one or more IPv4 collectors. The collectors aggregate the flow records and generate real-time or historical reports.

AppFlow provides visibility at the transaction level for HTTP, SSL, TCP, and SSL\_TCP flows. You can sample and filter the flow types that you want to monitor.

AppFlow use actions and policies to send records for a selected flow to specific set of collectors. An AppFlow action specifies which set of collectors will receive the AppFlow records. Policies, which are based on Advanced expressions can be configured to select flows for which flow records will be sent to the collectors specified by the associated AppFlow action.

To limit the types of flows, you can enable AppFlow for a virtual server. AppFlow can also provide statistics for the virtual server.

You can also enable AppFlow for a specific service, representing an application server, and monitor the traffic to that application server.

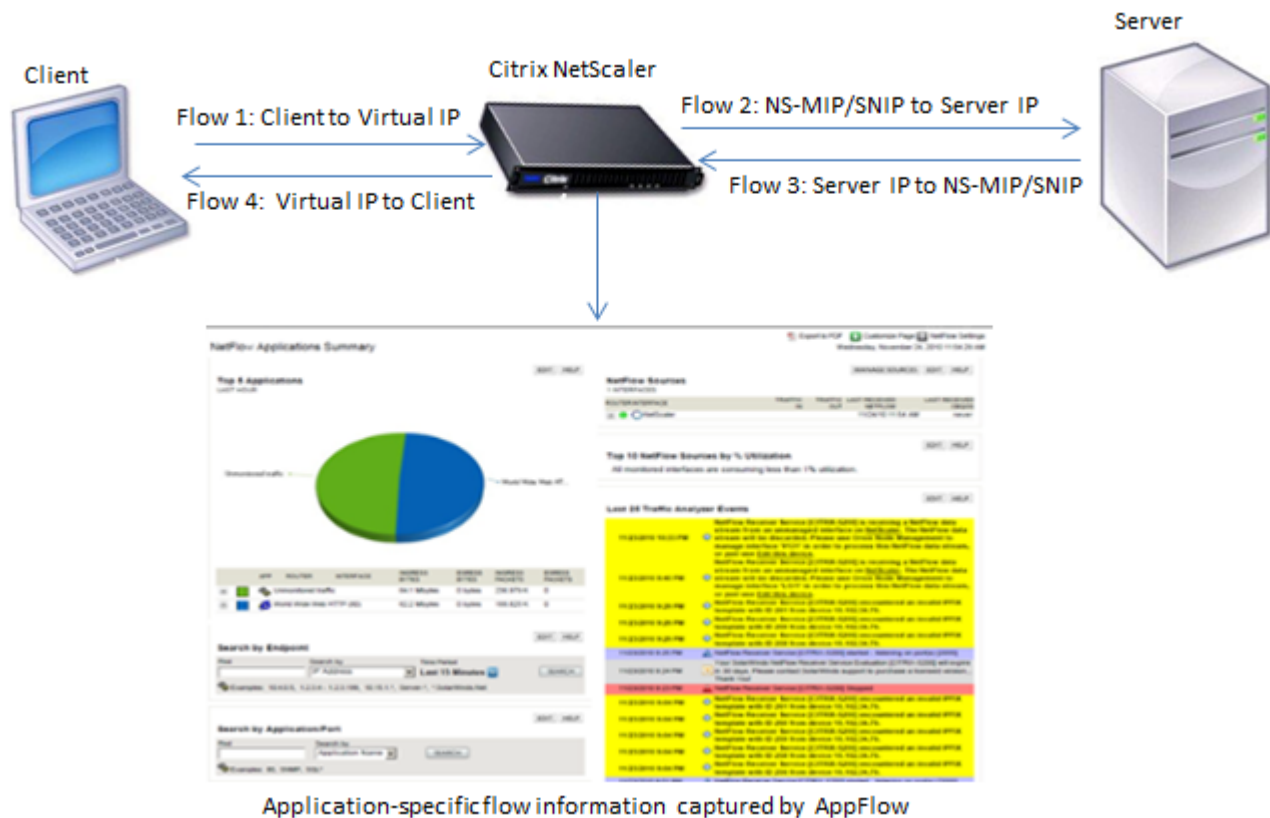
**Note:** This feature is supported only on NetScaler nCore builds.

## How AppFlow Works

In the most common deployment scenario, inbound traffic flows to a Virtual IP address (VIP) on the NetScaler appliance and is load balanced to a server. Outbound traffic flows from the server to a mapped or subnet IP address on the NetScaler and from the VIP to the client. A flow is a unidirectional collection of IP packets identified by the following five tuples: sourceIP, sourcePort, destIP, destPort, and protocol.

The following figure describes how the AppFlow feature works.

**Figure 7-1. NetScaler Flow Sequence**



As shown in the figure, the network flow identifiers for each leg of a transaction depend on the direction of the traffic.

The different flows that form a flow record are:

Flow1: <Client-IP, Client-Port, VIP-IP, VIP-port, Protocol>

Flow2: <NS-MIP/SNIP, NS-port, Server-IP, Server-Port, Protocol>

Flow3: <Server-IP, Server-Port, NS-MIP/SNIP, NS-Port, Protocol>

Flow4: <VIP-IP, VIP-port, Client-IP, Client-Port, Protocol>



To help the collector link all four flows in a transaction, AppFlow adds a custom `transactionID` element to each flow. For application-level content switching, such as HTTP, it is possible for a single client TCP connection to be load balanced to different backend TCP connections for each request. AppFlow provides a set of records for each transaction.

## Flow Records

AppFlow records contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of a flow, packet count, and byte count. AppFlow records also contain application-level information (such as HTTP URLs, HTTP request methods and response status codes, server response time, and latency) IPFIX flow records are based on templates that need to be sent before sending flow records.

## Templates

AppFlow defines a set of templates, one for each type of flow. Each template contains a set of standard Information Elements (IEs) and Enterprise-specific Information Elements (EIEs). IPFIX templates define the order and sizes of the Information Elements (IE) in the flow record. The templates are sent to the collectors at regular intervals, as described in RFC 5101.

A template can include the following EIEs:

### **transactionID**

An unsigned 32-bit number identifying an application-level transaction. For HTTP, this corresponds to a request and response pair. All flow records that correspond to this request and response pair have the same transaction ID. In the most common case, there are four unidirectional flow records that correspond to this transaction. If the NetScaler generates the response by itself (served from the integrated cache or by a security policy), there may be only two flow records for this transaction.

### **connectionID**

An unsigned 32-bit number identifying a layer-4 connection (TCP or UDP). The NetScaler flows are usually bidirectional, with two separate flow records for each direction of the flow. This information element can be used to link the two flows.

For the NetScaler, `connectionID` is an identifier for the connection data structure to track the progress of a connection. In an HTTP transaction, for instance, a given `connectionID` may have multiple `transactionID` elements corresponding to multiple requests that were made on that connection.

### **tcpRTT**

The round trip time, in milliseconds, as measured on the TCP connection. This can be used as a metric to determine the client or server latency on the network.

### **httpRequestMethod**

An 8-bit number indicating the HTTP method used in the transaction. An options template with the number-to-method mapping is sent along with the template.

**httpRequestSize**

An unsigned 32-bit number indicating the request payload size.

**httpRequestURL**

The HTTP URL requested by the client.

**httpUserAgent**

The source of incoming requests to the Web server.

**httpResponseStatus**

An unsigned 32-bit number indicating the response status code.

**httpResponseSize**

An unsigned 32-bit number indicating the response size.

**httpResponseTimeToFirstByte**

An unsigned 32-bit number indicating the time taken to receive the first byte of the response.

**httpResponseTimeToLastByte**

An unsigned 32-bit number indicating the time taken to receive the last byte of the response.

**flowFlags**

An unsigned 64-bit flag used to indicate different flow conditions.

## Configuring the AppFlow Feature

You configure AppFlow in the same manner as most other policy-based features. First, you enable the AppFlow feature. Then you specify the collectors to which the flow records are sent. After that, you define actions, which are sets of configured collectors. Then you configure one or more policies and associate a action to each policy. The policy tells the NetScaler appliance to select requests the flow records of which are sent to the associated action. Finally, you bind each policy either globally or to a specific vservers to put it into effect.

You can further set AppFlow parameters to specify the template refresh interval and to enable the exporting of httpURL, httpCookie, and httpReferer information. On each collector, you must specify the NetScaler IP address as the address of the exporter.

**Note:** For information about configuring the NetScaler as an exporter on the collector, see the documentation for the specific collector.

The configuration utility provides tools that help users define the policies and actions that determine exactly how the NetScaler appliance export records for a particular flow to a set of collectors(action.) The NetScaler command line provides a corresponding set of CLI-based commands for experienced users who prefer a command line.

## Enabling or Disabling the AppFlow Feature

To be able to use the AppFlow feature, you must first enable it.

### To enable or disable the AppFlow feature by using the NetScaler command line

At the NetScaler command prompt, type one of the following commands:

- ◆ `enable ns feature appflow`
- ◆ `disable ns feature appflow`

### To enable the AppFlow feature by using the configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Modes and Features**, click **Configure advanced features**.
3. In the **Configure Advanced Features** dialog box, select the **AppFlow** check box, and then click **OK**.
4. In the **Enable/Disable Feature(s)?** dialog box, click **Yes**.

## Specifying a Collector

A collector receives flow records generated by the NetScaler appliance. To be able to send flow records, you must specify at least one collector. You can specify up to four. However, you cannot export the same data to multiple collectors. You can remove unused collectors.

### To specify a collector by using the NetScaler command line

At the NetScaler command prompt, type the following commands to add a collector and verify the configuration:

- ◆ `add appflowCollector <name> -IPAddress <ipaddress> -port <port_number>`
- ◆ `show appflowCollector <name>`

#### Example

```
> add appflowCollector coll1 -IPAddress
10.102.29.251 -port 8000
Done

> show appflowCollector coll1

1)Collector name: coll1
   Collector IPv4 address: 10.102.29.251
   Collector UDP port: 8000
```

## To remove a collector by using the NetScaler command line

At the NetScaler command prompt, type:

```
rm appflowCollector <name>
```

## Parameters for specifying a collector

### name

Name of the collector to which to export data. Maximum characters: 255.

### ipaddress

The IPv4 address of the collector.

### port

The UDP port on which the collector is listening. Default port: 4739.

## To specify a collector by using the configuration utility

1. In the navigation pane, expand **AppFlow**, and then click **Collectors**.
2. In the details pane, click **Add**.
3. In the **Create AppFlow Collector** dialog box, specify values for the following parameters, which correspond to parameters described in "Parameters for specifying a collector" as shown:
  - **Name\***—name (cannot be changed for an existing collector)
  - **IP Address\***—ipaddress (cannot be changed for an existing collector)
  - **Port**—port (cannot be changed for an existing collector)

\*A required parameter
4. To remove a collector from the list, select the collector, and then click **Remove**.
5. Click **Create**, and then click **Close**.

## Configuring an AppFlow Action

An Appflow action is a set collectors, to which the flow records are sent if the associated Appflow policy matches.

## To configure an AppFlow action by using the NetScaler command line

At the NetScaler command prompt, type the following commands to configure an Appflow action and verify the configuration:

- ♦ **add appflow action** <name> --collectors <string> ... [-comment <string>]
- ♦ **show appflow action**

**Example**

```
> add appflow action apfl-act-collector-1-and-3 -
collectors collector-1 collector-3
Done

> show appflow action

1)      Name: apfl-act-collector-1
        Collectors: collector-1
        Hits: 0
        Action Reference Count: 2

2)      Name: apfl-act-collector-2-and-3
        Collectors: collector-2, collector-3
        Hits: 0
        Action Reference Count: 1

3)      Name: apfl-act-collector-1-and-3
        Collectors: collector-1, collector-3
        Hits: 0
        Action Reference Count: 1

Done
```

## To modify or remove an AppFlow action by using the NetScaler command line

- ◆ To modify an AppFlow action, type the **set appflow action** command, the name of the action, and the parameters to be changed, with their new values.
- ◆ To remove an AppFlow action, type the **rm appflow action** command and the name of the action.

## Parameters for configuring an AppFlow action

**name**

A name for your new action, or the name of the existing action you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (\_) symbols.

**collectors**

The name of a set of configured collectors.

**comment**

Any comments that you may want to associate with the policy. Maximum length: 255 characters. To include spaces in a comment that you type on the NetScaler command line, enclose the entire comment inside quotation marks. The quotation marks do not become part of the comment. They are not required if you use the configuration utility.

## To configure an AppFlow action by using the configuration utility

1. In the navigation pane, expand **AppFlow**, and then click **Actions**.
2. In the details pane, do one of the following:
  - To create a new action, click **Add**.
  - To modify an existing action, select the action, and then click **Open**.
3. In the **Add AppFlow Action** or **Configure AppFlow Action** dialog box, type a name for the new action or the name of an existing action, respectively. For allowed characters, see "Parameters for configuring an AppFlow action."
4. Do one of the following to associate collectors with the action:
  - If the collectors that you want are listed, click the corresponding check boxes.
  - If you want to specify all the collectors, click **Activate All**.
  - If you want to specify a new collector, click **Add**.
5. Click **Create** or **OK**, depending on whether you are creating a new action or modifying an existing action.
6. Click **Close**. A message appears in the status bar, stating that the configuration has been successfully implemented.

## Configuring an AppFlow Policy

After you configure an AppFlow action, you must next configure an AppFlow policy. An AppFlow policy is based on a rule, which consists of one or more expressions.

**Note:** For creating and managing AppFlow policies, the configuration utility provides assistance that is not available at the NetScaler command line.

### To configure an AppFlow policy by using the NetScaler command line

At the NetScaler command prompt, type the following command to add an AppFlow policy and verify the configuration:

- ♦ **add appflow policy** <name> <expression> <action>
- ♦ **show appflow policy** <name>

#### Example

```
> add appflow policy apfl-pol-tcp-dsprt
client.TCP.DSTPORT.EQ(22) apfl-act-collector-1-
and-3
Done
> show appflow policy
```

```
1)      Name: apfl-pol-myPolicy5
        Hits: 0
        Undef Hits: 0
        Active: Yes

2)      Name: apfl-pol-myPolicy10
        Hits: 0
        Undef Hits: 0
        Active: Yes

3)      Name: apfl-pol-myPOL30
        Hits: 0
        Undef Hits: 0
        Active: Yes

4)      Name: apfl-pol-myPolicy50
        Hits: 0
        Undef Hits: 0
        Active: No

5)      Name: apfl-pol-tcp-dsprt
        Hits: 0
        Undef Hits: 0
        Active: No

Done
```

## To modify or remove an AppFlow policy by using the NetScaler command line

- ◆ To modify an AppFlow policy, type the **set appflow policy** command, the name of the policy, and the parameters to be changed, with their new values.
- ◆ To remove an AppFlow policy, type the **rm appflow policy** command and the name of the policy.

## Parameters for configuring an AppFlow policy

### name

A name for the policy, or the name of the existing policy you want to modify. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (\_) symbols.

### rule

The expression that defines the rule for this policy. The expression can be a simple expression or a complex expression that contains several expressions in structured relationship to one another. Expressions are written in the NetScaler Policy Infrastructure (PI) language. For more information about PI, see the *Citrix NetScaler Policy Configuration and Reference Guide* at <http://support.citrix.com/article/CTX128673>.

### action

The name of the action associated with the policy.

### comment

Any comments that you may want to associate with the policy. Maximum length: 255 characters. To include spaces in a comment that you type on the NetScaler command line, enclose the entire comment inside quotation marks. The quotation marks do not become part of the comment. They are not required if you use the configuration utility.

## To configure an AppFlow policy by using the configuration utility

1. In the navigation pane, expand **AppFlow**, and then click **Policies**.
2. In the details pane, do one of the following:
  - To create a new policy, click **Add**.
  - To modify an existing policy, select the policy, and then click **Open**.
3. In the **Create AppFlow Policy** or **Configure AppFlow Policy** dialog box, type or select values for the following parameters, which correspond to parameters described in "Parameters for configuring an AppFlow policy" as shown:
  - Name\*—name
  - Action\*—action
  - Expression\*—rule (You can add the expression in any of three ways. (1) You can click **Add** and choose an existing expression in the **Frequently Used Expressions** drop-down list. (2) You can type the expression directly into the supplied text box. For brief help and prompts, while the cursor is in the text box, hold down the **CTRL** key while you press the **Space** bar. (3) You can use the **Add Expression** dialog box, as described in "To add an expression by using the **Add Expression** dialog box.")
  - Comments—comment
4. Click **Create** or **OK**, depending on whether you are creating a new policy or modifying an existing policy.
5. Click **Close**. A message appears in the status bar, stating that the configuration has been successfully implemented.

## To add an expression by using the Add Expression dialog box

1. In the **Add Expression** dialog box, in the first list box choose the first term for your expression.

### HTTP

The HTTP protocol. Choose this if you want to examine some aspect of the request that pertains to the HTTP protocol.

### SYS

The protected Web site(s). Choose this if you want to examine some aspect of the request that pertains to the recipient of the request.



**CLIENT**

The computer that sent the request. Choose this if you want to examine some aspect of the sender of the request.

When you make your choice, the rightmost list box lists appropriate terms for the next part of your expression.

2. In the second list box, choose the second term for your expression.  
The choices depend upon which choice you made in the previous step, and are appropriate to the context. After you make your second choice, the **Help** window below the **Construct Expression** window (which was blank) displays help describing the purpose and use of the term you just chose.
3. Continue choosing terms from the list boxes that appear to the right of the previous list box, or typing strings or numbers in the text boxes that appear to prompt you to enter a value, until your expression is finished. For more information about the PI expressions language and creating expressions for AppFlow policies, see the *Citrix NetScaler Policy Configuration and Reference Guide*. For a link to the guide, see the [Documentation Library](#).

## Binding an AppFlow Policy

To put a policy into effect, you must bind it either globally, so that it applies to all traffic that flows through the NetScaler, or to a specific virtual server, so that the policy applies only to the traffic related to that virtual server.

When you bind a policy, you assign it a priority. The priority determines the order in which the policies you define are evaluated. You can set the priority to any positive integer.

In the NetScaler operating system, policy priorities work in reverse order—the higher the number, the lower the priority. For example, if you have three policies with priorities of 10, 100, and 1000, the policy assigned a priority of 10 is performed first, then the policy assigned a priority of 100, and finally the policy assigned an order of 1000.

You can leave yourself plenty of room to add other policies in any order, and still set them to evaluate in the order you want, by setting priorities with intervals of 50 or 100 between each policy when you globally bind it. You can then add additional policies at any time without having to change the priority of an existing policy.

For additional information about binding policies on the NetScaler, see the *Citrix NetScaler Traffic Management Guide* at <http://support.citrix.com/article/CTX128670>.

### To globally bind an AppFlow policy by using the NetScaler command line

At the NetScaler command prompt, type the following command to globally bind an AppFlow policy and verify the configuration:

- ♦ **bind appflow global** <policyName> <priority> [<gotoPriorityExpression [-type <type>] [-invoke (<labelType> <labelName>)]
- ♦ **show appflow global**

## To bind an AppFlow policy to a specific virtual server by using the NetScaler command line

At the NetScaler command prompt, type the following command to bind an appflow policy to a specific virtual server and verify the configuration:

```
bind lb vserver <name> -policyname <policy_name> -priority <priority>
```

## Parameters for binding an AppFlow policy

### name

The name of the virtual server to which you are binding the AppFlow policy.

### policyname

The name of the AppFlow policy that you want to bind.

### priority

A number specifying the priority assigned to this policy. The lower the number, the higher the priority. The priority determines the order in which policies are evaluated, allowing the NetScaler to evaluate the most specific policy first, and more general policies in descending order, finishing with the most general policy.

### gotoPriorityExpression

The priority of the next policy that should be evaluated if this policy matches. If set to END, this parameter halts the policy evaluation process after evaluation of the current policy. If you are careful to assign your policy priorities in the right order, you can use this parameter to skip over policies in the event that the current policy matches, and go directly to a specific policy.

### type

Bind point, specifying where to bind the policy.

### invoke

Invoke flag.

### labelType

Type of policy label invocation.

### labelName

Name of the label to invoke if the current policy rule evaluates to TRUE.

## To globally bind an AppFlow policy by using the configuration utility

1. In the navigation pane, expand **AppFlow**.
2. On the **AppFlow** page, click **Policy Manager**.
3. In the **AppFlow Policy Manager** dialog box, in the **Bind Points** menu, select **Default Global**.
4. Click **Insert Policy** to insert a new row and display a drop-down list of all unbound AppFlow policies.

5. Click one of the policies on the list. That policy is inserted into the list of globally bound AppFlow policies.
6. Click **Apply Changes**.
7. Click **Close**. A message appears in the status bar, stating that the configuration has been successfully implemented.

### To bind an AppFlow policy to a specific virtual server by using the configuration utility

1. In the navigation pane, expand **Load Balancing**, and then click **Virtual Servers**.
2. On the **Load Balancing Virtual Servers** page, select the virtual server to which you want to bind the AppFlow policy, and then click **Open**.
3. In the **Configure Virtual Server (Load Balancing)** dialog box, select the **Policies** tab to display the policies bound to that particular virtual server.
4. Click **Insert Policy** to insert a new row and display a drop-down list of all unbound AppFlow policies.
5. From the drop-down list that appears under **Policy Name**, select the policy that you want to bind to this virtual server.
6. Click **OK**, and then click **Close**. A message appears in the status bar, stating that the configuration has been successfully implemented

## Enabling AppFlow for Virtual Servers

If you want to monitor only the traffic through certain virtual servers, enable AppFlow specifically for those virtual servers. You can enable AppFlow for load balancing, content switching, cache redirection, SSL VPN, GSLB, and authentication virtual servers.

### To enable AppFlow for a virtual server by using the NetScaler command line

At the NetScaler command prompt, type:

```
set <feature_name> vsserver <vServerName> <protocol> <IPAddress> <port> -  
appflowLog ENABLED
```

#### Example

```
set cs vsserver Vserver-CS-1 HTTP 10.102.29.161 80 -  
appflowLog ENABLED
```

### To enable AppFlow for a virtual server by using the configuration utility

1. In the navigation pane, expand the feature node for which you want to enable AppFlow, and then click **Virtual Servers**.

For example, expand **Content Switching** to enable AppFlow for a content switching virtual server, and then click **Virtual Servers**.

2. In the details pane, do one of the following:
  - To enable AppFlow for a new virtual server, click **Add**.
  - To enable AppFlow for an existing virtual server, select the virtual server, and then click **Open**.
3. In the **Create Virtual Server** (feature\_name) dialog box or the **Configure Virtual Server** (feature\_name) dialog box, select the **AppFlow Logging** check box.
4. Click **Create** or **OK**, and then click **Close**.

## Enabling AppFlow for a Service

You can enable AppFlow for services that are to be bound to the load balancing virtual servers.

### To enable AppFlow for a service by using the NetScaler command line

At the NetScaler command prompt, type:

```
set service<name> -appflowLog ENABLED
```

### To enable AppFlow for a service by using the configuration utility

1. In the navigation pane, expand **Load Balancing**, and then click **Services**.
2. In the details pane, do one of the following:
  - To enable AppFlow for a new service, click **Add**.
  - To enable AppFlow for an existing service, select the service, and then click **Open**.
3. In the **Create Service** or the **Configure Service** dialog box, select the **AppFlow Logging** check box.
4. Click **OK**, and then click **Close**.

## Setting the AppFlow Parameters

You can set AppFlow parameters to customize the exporting of data to the collectors.

### To set the AppFlow Parameters by using the NetScaler Command Line

At the NetScaler command prompt, type the following commands to set the AppFlow parameters and verify the settings:

- ◆ **set appflowParam** [-templateRefresh <secs>] [-appnameRefresh <secs>] [-flowRecordInterval <secs>] [-udpPmtu <positive\_integer>] [-httpUrl ( ENABLED | DISABLED )] [-httpCookie ( ENABLED | DISABLED )] [-httpReferer ( ENABLED | DISABLED )] [-httpMethod ( ENABLED | DISABLED )] [-httpHost ( ENABLED | DISABLED )] [-httpUserAgent ( ENABLED | DISABLED )] [-clientTrafficOnly ( YES | NO)]
- ◆ **show appflowParam**

**Example**

```
> set appflowParam -templateRefresh 240 -udpPmtu
128 -httpUrl enabled
Done

> show appflowparam
AppFlow parameters
IPFIX template refresh interval: 600 seconds
IPFIX UDP Path MTU: 1472 bytes
HTTP URL logging: DISABLED
HTTP cookie logging: DISABLED
HTTP referer logging: DISABLED
HTTP method logging: ENABLED
HTTP host logging: ENABLED
HTTP user-agent logging: ENABLED
Log only client-side traffic: NO
Done
```

## To return AppFlow parameters to their default values by using the NetScaler command line

Type the **unset appflowParam** command and the names of the parameters to be returned to the default values.

## AppFlow Parameters

### templateRefresh

The refresh interval, in seconds, at which to export the template data. Because data transport is in the UDP protocol, the templates must be resent at regular intervals. Minimum value: 60. Maximum value: 3600. Default: 600.

### appnameRefresh

Interval at which Appnames are sent to the configured collectors, in seconds. Minimum value: 60. Maximum value: 3600. Default: 600.

### flowRecordInterval

Interval at which flow records are sent to the configured collectors, in seconds. Minimum value: 60. Maximum value: 3600. Default: 600.

### udpPmtu

The maximum length of the UDP datagram. Default: 1472.

### httpUrl

The http URL received by the NetScaler appliance from the client. Possible values: ENABLED, DISABLED. Default: DISABLED.

**httpCookie**

Include the cookie that was in the HTTP request received by the NetScaler appliance from the client. Possible values: ENABLED, DISABLED. Default: DISABLED.

**httpReferer**

Include the Web page that was last visited by the client. Possible values: ENABLED, DISABLED. Default: DISABLED.

**httpMethod**

Include the method that was specified in the HTTP request received by the NetScaler appliance from the client. Possible values: ENABLED, DISABLED. Default: DISABLED.

**httpHost**

Include the host identified in the HTTP request received by the NetScaler appliance from the client. Possible values: ENABLED, DISABLED. Default: DISABLED.

**httpUserAgent**

Include the client application through which the HTTP request was received by the NetScaler appliance. Possible values: ENABLED, DISABLED. Default: DISABLED.

**clientTrafficOnly**

Generate AppFlow records only for the traffic from the client. Possible values: YES, NO. Default: NO.

## To set the AppFlow parameters by using the configuration utility

1. In the navigation pane, click **AppFlow**.
2. On the **AppFlow** landing page, under **Settings**, click **Change AppFlow Settings**.
3. In the **Configure AppFlow Settings** dialog box, specify values for the following parameters, which correspond to parameters described in "AppFlow Parameters" as shown:
  - **Template Refresh Interval**—templateRefresh
  - **AppName Refresh Interval**—appnameRefresh
  - **Flow Record Export Interval**—flowRecordInterval
  - **HTTP URL**—httpUrl
  - **HTTP Cookie**—httpCookie
  - **HTTP Referer**—httpReferer
  - **HTTP Method**—httpMethod
  - **HTTP Host**—httpHost
  - **HTTP User-Agent**—httpUserAgent
  - **Template Refresh Interval**—templateRefresh
  - **UDP Maximum Transmission Unit**—udpPmtu
4. Click **OK**, and then click **Close**.

---

## Chapter 8

# Reporting Tool

### Topics:

- [\*Using the Reporting Tool\*](#)
- [\*Stopping and Starting the Data Collection Utility\*](#)

Use the Citrix® NetScaler® Reporting tool to view NetScaler performance statistics data as reports. Statistics data are collected by the nscollect utility and are stored in a database. When you want to view certain performance data over a period of time, the Reporting tool pulls out specified data from the database and displays them in charts.

Reports are a collection of charts. The Reporting tool provides built-in reports as well as the option to create custom reports. In a report, you can modify the charts and add new charts. You can also modify the operation of the data collection utility, nscollect, and stop or start its operation.

## Using the Reporting Tool

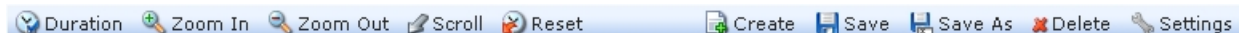
The Reporting tool is a Web-based interface accessed from the Citrix® NetScaler® appliance. Use the Reporting tool to display the performance statistics data as reports containing graphs. In addition to using the built-in reports, you can create custom reports, which you can modify at any time. Reports can have between one and four charts. You can create up to 256 custom reports.

### To invoke the Reporting tool

1. Use the Web browser of your choice to connect to the IP address of the NetScaler (for example, `http://10.102.29.170/`).  
The Web Logon screen appears.
2. In the **User Name** text box, type the user name assigned to the NetScaler.
3. In the **Password** text box, type the password.
4. In the **Start in** drop-down box, select **Reporting**.
5. Click **Login**.

The following screen shots show the report toolbar and the chart toolbar, which are frequently referenced in this documentation.

**Figure 8-1. Report Toolbar**



**Figure 8-2. Chart Toolbar**



## Working with Reports

You can plot and monitor statistics for the various functional groups configured on the NetScaler over a specified time interval. Reports enable you to troubleshoot or analyze the behavior of your appliance. There are two types of reports: built-in reports and custom reports. Report content for built-in or custom reports can be viewed in a graphical format or a tabular format. The graphical view consists of line, area, and bar charts that can display up to 32 sets of data (counters). The tabular view displays the data in columns and rows. This view is useful for debugging error counters.

The default report that is displayed in the Reporting tool is CPU vs. Memory Usage and HTTP Requests Rate. You can change the default report view by displaying the report you want as your default view, and then clicking **Default Report**.

Reports can be generated for the last hour, last day, last week, last month, last year, or you can customize the duration.

You can do the following with reports:



- ◆ Toggle between a tabular view of data and a graphical view of data.
- ◆ Change the graphical display type, such as bar chart or line chart.
- ◆ Customize charts in a report.
- ◆ Export the chart as an Excel comma-separated value (CSV) file.
- ◆ View the charts in detail by zooming in, zooming out, or using a drag-and-drop operation (scrolling).
- ◆ Set a report as the default report for viewing whenever you log on.
- ◆ Add or remove counters.
- ◆ Print reports.
- ◆ Refresh reports to view the latest performance data.

## Using Built-in Reports

The Reporting tool provides built-in reports for frequently viewed data. Built-in reports are available for the following seven functional groups: System, Network, SSL, Compression, Integrated Cache, Access Gateway, and Application Firewall. By default, the built-in reports are displayed for the last day. However, you can view the reports for the last hour, last week, last month, or last year.

**Note:** You cannot save changes to built-in reports, but you can save a modified built-in report as a custom report.

### To display a built-in report

1. In the left pane of the Reporting tool, under **Built-in Reports**, expand a group (for example, **SSL**).
2. Click a report (for example, **SSL > All Backend Ciphers**).

## Creating and Deleting Reports

You can create your own custom reports and save them with user-defined names for reuse. You can plot different counters for different groups based on your requirements. You can create up to 256 custom reports.

You can either create a new report or save a built-in report as a custom report. By default, a newly created custom report contains one chart named **System Overview**, which displays the **CPU Usage** counter plotted for the last day. You can customize the interval and set the data source and time zone from the report toolbar. Within a report, you can use the chart toolbars to add, modify, or delete charts, as described in [Working with Charts](#) on page 188.

By default, newly created custom reports contain one chart named **System Overview** that displays a **CPU Usage** counter plotted for the last day.

### To create a custom report

1. In the Reporting tool, on the report toolbar, click **Create**, or if you want to create a new custom report based on an existing report, open the existing report, and then click **Save As**.
2. In **Report Name** box, type a name for the custom report.
3. Do one of the following:
  - To add the report to an existing folder, in **Create in** or **Save in**, click the down arrow to choose an existing folder, and then click **OK**.
  - To create a new folder to store the report, click the **Click to add folder** icon, in **Folder Name**, type the name of the folder, and in **Create in**, specify where you want the new folder to reside in the hierarchy, and then click **OK**.

**Note:** You can create up to 128 folders.

### To delete a custom report




1. In the left pane of the Reporting tool, next to **Custom Reports**, click the **Click to manage custom reports** icon.
2. Select the check box that corresponds with the report you want to delete, and then click **Delete**.




**Note:** When you delete a folder, all the contents of that folder are deleted.

### Modifying the Time Interval

By default, built-in reports display data for the last day. However, if you want to change the time interval for a built-in report, you can save the report as a custom report. The new interval applies to all charts in the report. The following table describes the time-interval options.

**Table 8-1.** Time Intervals

Time interval	Displays
 Last Hour	Statistics data collected for the last hour.
 Last Day	Statistics data collected for the last day (24 hours).
 Last Week	Statistics data collected for the last week (7 days).

Time interval	Displays
 Last Month	Statistics data collected for the last month (31 days).
 Last Year	Statistics data collected for the last year (365 days).
 Custom	Statistics data collected for a time period that you are prompted to specify.

### To modify the time interval

1. In the left pane of the Reporting tool, click a report.
2. On the report toolbar, click **Duration**, and then click a time interval.

## Setting the Data Source and Time Zone

You can retrieve data from different data sources to display them in the reports. You can also define the time zone for the reports and apply the currently displayed report's time selection to all the reports, including the built-in reports.

### To set the data source and time zone

1. In the **Reporting tool**, on the report toolbar, click **Settings**.
2. In the **Settings** dialog box, in **Data Source**, select the data source from which you want to retrieve the counter information.
3. Do one or both of the following:
  - If you want the tool to remember the time period for which a chart is plotted, select the **Remember time selection for charts** check box.
  - If you want the reports to use the time settings of your NetScaler appliance, select the **Use Appliance's time zone** check box.

## Exporting and Importing Custom Reports

You can share reports with other NetScaler administrators by exporting reports. You can also import reports.

### To export or import custom reports

1. In the left pane of the Reporting tool, next to **Custom Reports**, click the **Click to manage custom reports** icon.
2. Select the check box that corresponds with the report you want to export or import, and then click **Export** or **Import**.

**Note:** When you export the file, it is exported in a .gz file format.

## Working with Charts

Use charts to plot and monitor counters or groups of counters. You can include up to four charts in one report. In each chart, you can plot up to 32 counters. The charts can use different graphical formats (for example, area and bar). You can move the charts up or down within the report, customize the colors and visual display for each counter in a chart, and delete a chart when you do not want to monitor it.

In all report charts, the horizontal axis represents time and the vertical axis represents the value of the counter.

### Adding a Chart

When you add a chart to a report, the **System Overview** chart appears with the **CPU Usage** counter plotted for the last one day. To plot a different group of statistics or select a different counter, see [Modifying a Chart](#) on page 188.

**Note:** If you add charts to a built-in report, and you want to retain the report, you must save the report as a custom report.

Use the following procedure to add a chart to a report.

#### To add a chart to a report

1. In the left pane of the **Reporting tool**, click a report.
2. Under the chart where you want to add the new chart, click the **Add** icon.

### Modifying a Chart

You can modify a chart by changing the functional group for which the statistics are displayed and by selecting different counters.

#### To modify a chart

1. In the left pane of the Reporting tool, click a report.
2. Under the chart that you want to modify, click **Counters**.
3. In the dialog box that appears, in the **Title** box, type a name for the chart.
4. Next to **Plot chart for**, do one of the following:
  - To plot counters for global counters, such as Integrated Cache and Compression, click **System global statistics**.
  - To plot entity counters for entity types, such as Load Balancing and GSLB, click **System entities statistics**.
5. In **Select group**, click the desired entity.

6. Under **Counters**, in **Available**, click the counter name(s) that you want to plot, and then click the > button.
7. If you selected **System entities statistics** in step 4, on the **Entities** tab, under **Available**, click the entity instance name(s) you want to plot, and then click the > button.
8. Click **OK**.

## Viewing a Chart

You can specify the graphical formats of the plotted counters in a chart. Charts can be viewed as line charts, spline charts, step-line charts, scatter charts, area charts, bar charts, stacked area charts, and stacked bar charts. You can also zoom in, zoom out, or scroll inside the plot area of a chart. You can zoom in or out for all data sources for 1 hour, 1 day, 1 week, 1 month, 1 year, and 3 years.

Other options for customizing the view of a chart include customizing the axes of the charts, changing the background and edge color of the plot area, customizing the color and size of the grids, and customizing the display of each data set (counter) in a chart.

Data set numbers, such as Data Set 1, correspond to the order in which the counters in your graph are displayed at the bottom of the chart. For example, if **CPU usage** and **Memory usage** are displayed in first and second order at the bottom of the chart, **CPU usage** is equal to **Data Set 1** and **Memory usage** is equal to **Data Set 2**.

Whenever you modify a built-in report, you need to save the report as a custom report to retain your changes.

### To change the graph type of a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart you want to view, on the chart toolbar, click **Customize**.
3. On the **Chart** tab, under **Category**, click **Plot type**, and then click the graph type you want to display for the chart. If you want to display the graph is 3D, select the **Use 3D** check box.

### To refocus a chart with detailed data

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, on the report toolbar, click **Zoom In**, and do one or both of the following:
  - To refocus the chart to display data for a specific time window, drag and drop the cursor from the start time to the end time. For example, you can view data for a one-hour period on a certain day.
  - To refocus the chart to display data for a data point, simply click once on chart where you want to zoom in and get more detailed information.

3. Once you have the desired range of time for which you want to view detailed data, on the report toolbar, click **Tabular View**. Tabular view displays the data in numeric form in rows and columns.

### To view numeric data for a graph

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, on the report toolbar, click **Tabular View**. To return to the graphical view, click **Graphical View**.

**Note:** You can also view the numeric data in the graphical view by hovering your cursor over the notches in the gridlines.

### To scroll through time in a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, on the report toolbar, click **Scroll**, and then click inside the chart and drag the cursor in the direction for which you want to see data for a new time period. For example, if you want to view data in the past, click and drag to the left.

### To change the background color and text color of a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart for which you want to customize the axes, click **Customize**.
3. On the **Chart** tab, under **Category**, click one or more of the following:
  - To change the background color, click **Background Color**, and then select the options for color, transparency, and effects.
  - To change the text color, click **Text Color**, and then select the options for color, transparency, and effects.

### To customize the axes of a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart for which you want to customize the axes, click **Customize**.
3. On the **Chart** tab, under **Category**, click one or more of the following:
  - To change the scale of the left y-axis, click **Left Y-Axis**, and then select the scale you want.
  - To change the scale of the right y-axis, click **Right Y-Axis**, in **Data set to plot**, select the data set, and then select the scale you want.

**Note:** The data set numbers, such as Data Set 1, correspond to the order in which the counters in your graph are displayed at the bottom of the chart. For

example, if **CPU usage** and **Memory usage** are displayed in first and second order at the bottom of the chart, **CPU usage** is equal to **Data Set 1** and **Memory usage** is equal to **Data Set 2**.

- To plot each data set in its own hidden y-axis, click **Multiple Axes**, and then click **Enable**.

### To change the background color, edge color, and gridlines for a plot area of a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart for which you want to customize the plot area, click **Customize**.
3. On the **Plot Area** tab, under **Category**, click one or more of the following:
  - To change the background color and edge color of the chart, click **Background Color** and **Edge Color**, and then select the options for color, transparency, and effects.
  - To change the horizontal or vertical grids of the chart, click **Horizontal Grids** or **Vertical Grids**, and then select the options for displaying the grids, grid width, grid color, transparency, and effects.

### To change the color and graph type of a data set

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart for which you want to customize the display of the data set (counters), click **Customize**.
3. On the **Data Set** tab, in **Select Data Set**, select the data set (counter) for which you want to customize the graphical display.

**Note:** The data set numbers, such as Data Set 1, correspond to the order in which the counters in your graph are displayed at the bottom of the chart. For example, if **CPU usage** and **Memory usage** are displayed in first and second order at the bottom of the chart, **CPU usage** is equal to **Data Set 1** and **Memory usage** is equal to **Data Set 2**.

4. Under **Category**, do one of more of the following:
  - To change the background color, click **Color**, and then select the options for color, transparency, and effects.
  - To change the graph type, click **Plot type**, and then select the graph type you want to display for the data set. If you want to display the graph as 3D, select the **Use 3D** check box.

### Exporting Chart Data to Excel

For further data analysis, you can export charts to Excel in a comma-separated value (CSV) format.

#### To export chart data to Excel

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart with the data you want to export to Excel, click **Export**.

### Deleting a Chart

If you do not want to use a chart, you can remove it from the report. You can permanently remove charts from custom reports only. If you delete a chart from a built-in report and want to retain the changes, you need to save the report as a custom report.

#### To delete a chart

1. In the left pane of the Reporting tool, select a report.
2. In the right pane, under the chart that you want to delete, click the **Delete** icon.

## Examples

### To display the trend report for CPU usage and memory usage for the last week

1. In the left pane of the Reporting tool, under **Built-in Reports**, expand **System**.
2. Click the report **CPU vs. Memory Usage and HTTP Requests Rate**.
3. In the right pane, on the report toolbar, click **Duration**, and then click **Last Week**.

### To compare the bytes received rate and the bytes transmitted rate between two interfaces for the last week

1. In the right pane, on the report toolbar, click **Create**.
2. In the **Report Name** box, type a name for the custom report (for example, `Custom_Interfaces`), and then click **OK**.  
The report is created with the default **System Overview** chart, which displays the **CPU Usage** counter plotted for the last hour.
3. Under **System Overview**, on the chart toolbar, click **Counters**.
4. In the counter selection pane, in **Title**, type a name for the chart (for example, `Interfaces bytes data`).
5. In **Plot chart for**, click **System entities statistics**, and then in **Select Group**, select **Interface**.
6. On the **Entities** tab, click the interface name(s) you want to plot (for example, `1/1` and `1/2`), and then click the **>** button.
7. On the **Counters** tab, click **Bytes received (Rate)** and **Bytes transmitted (Rate)** and then click the **>** button.



8. Click **OK**.
9. On the report toolbar, click **Duration**, and then click **Last Week**.

## Stopping and Starting the Data Collection Utility

The performance data is stored in different data sources on the Citrix® NetScaler® appliance. The default data source is `/var/log/db/default`. You can create up to 32 data sources.

The data collection utility `nscollect` retrieves data from the NetScaler and updates the data source. This utility runs automatically when you start the NetScaler. It creates a database for global counters at `/var/log/db/<DataSourceName>`. The entity-specific databases are created based on the entities configured on the NetScaler. A specific folder is created for each entity type in

```
/var/log/db/<DataSourceName/EntityNameDB>
```

Before creating a database for an entity, `nscollect` allocates a unique number to the entity and creates the database based on that number. It retrieves all the counters available for a group. However, there is a limit on the number of different entities that `nscollect` can retrieve, as described in the following table.

**Table 8-2. Limits on Entity Numbers Retrieved by nscollect**

Entity name	Limit
Content Switching Virtual Servers	100
Cache Redirection Virtual Servers	50
DOS Policies	100
GSLB Domains	100
GSLB Services	100
GSLB Sites	32
GSLB Virtual Servers	100
Interfaces	8
LB Virtual Servers	100
ACLs	100

Entity name	Limit
ACL6	50
Priority Queuing Policies	100
RNAT IP Addresses	100
SureConnect Policies	100
Services	250
Service Groups	100
System CPU	8
VLAN	25
VPN Virtual Servers	5

The `nscollect` utility retrieves *n* number of entity counters and creates the entity database. If the first *n* counters change in the subsequent fetch, the database stores more than *n* entries for that entity type. However, you need to delete the unused entity counters manually.

**Note:** The Reporting tool supports only numerical counters.

By default, `nscollect` retrieves data at every 5-minute interval. Data is maintained in 5-minute granularity for one day, hourly for the last 30 days, and daily for three years.

When you start the NetScaler, the `nscollect` utility automatically starts. However, if data is not updated accurately, or there is corrupted data displayed in the reports, you can stop and then restart the utility. You may also want to stop `nscollect` to back up the databases or to create a new data source.

## To stop `nscollect`

At a NetScaler command prompt, type the following:

```
/netscaler/nscollect stop
```

You can start `nscollect` on either the local system or a remote system.

## To start `nscollect` on the local system

At a NetScaler command prompt, type the following:

```
/netscaler/nscollect start
```

## To start nscollect on the remote system

At a NetScaler command prompt, type the following:

```
/netscaler/nscollect start -U NS_IP:UserName:Password -ds DataSourceName
```

### **Example**

```
/netscaler/nscollect start -U  
10.102.29.170:nsroot:nsroot -ds default
```